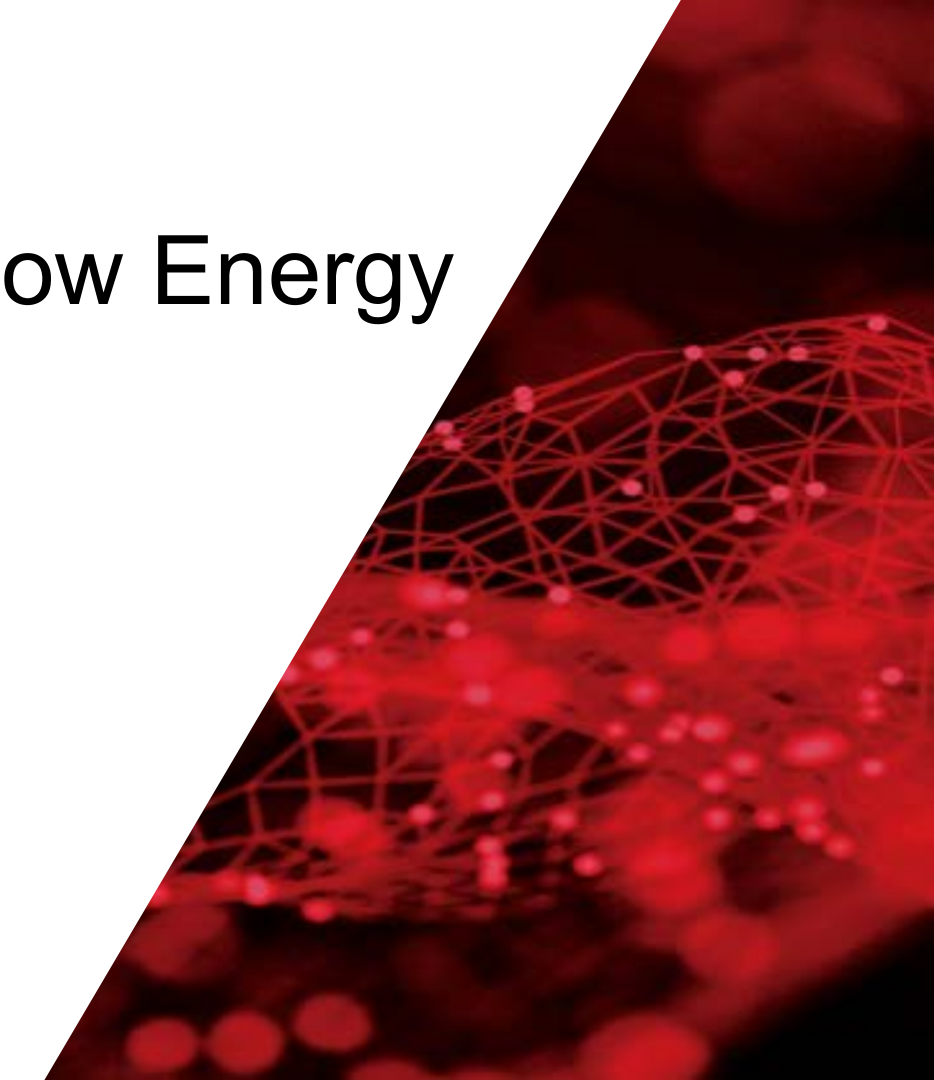
Breaking Bluetooth Low Energy

Maxine Filcher
Security Consultant



IOActive®

Agenda

- Part 1
  - BLE Protocol Basics
- Part 2
  - Vulnerabilities
- Part 3
  - Code

CAUTION

ALL YOUR RF ARE BELONG TO US!

Your proximity to this device constitues consent to be monitored on all applicable parts of the electro-magnetic spectrum.
You have no chance for privacy make your time.

wirelessvillage.ninja WIRELESS VILLAGE www.wctf.us

Whoami

- Maxine Filcher
- Security Consultant with IOActive
- US Army Veteran
- B.S. Info Assurance & Cybersecurity
  - Minor: Law & Policy
- SANS Women's Academy 2018 Cohort
- GSEC, GCIH, GPEN
  - maxine.filcher@ioactive.com
  - @FreqyXin

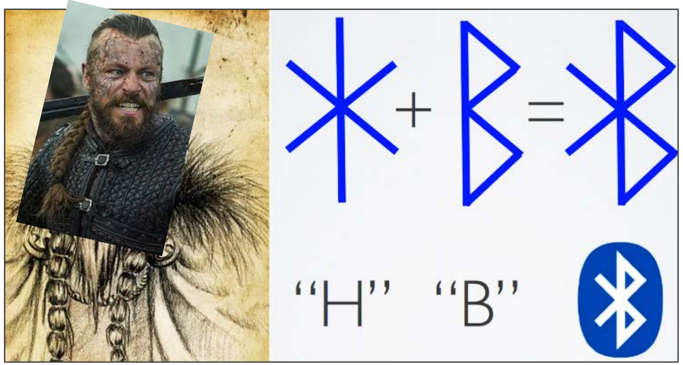
Disclaimer:

I am not a Bluetooth Developer
This is not a comprehensive class on Bluetooth

Part I

A Quick History

- Herald “Bluetooth”
- King of Norway and Denmark



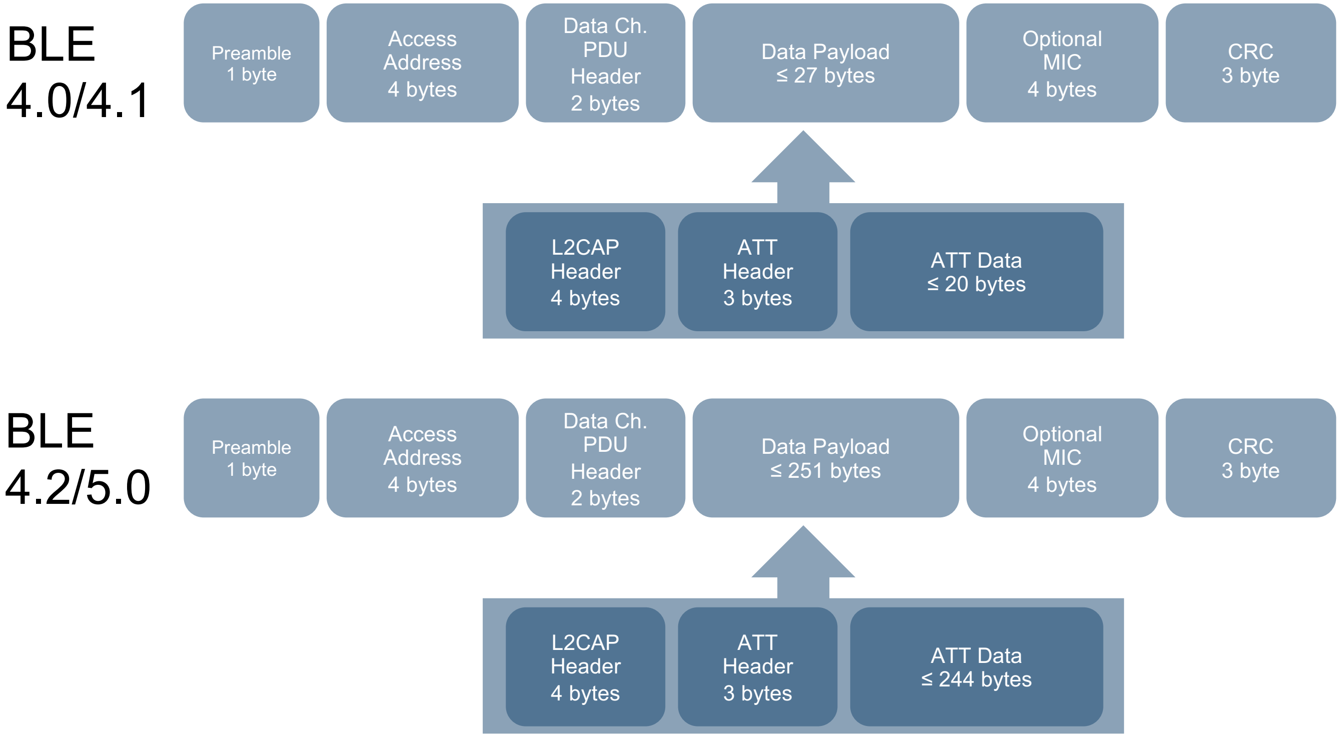
- Hedy Lamarr
- 1914-2000
- Frequency Hopping Spread Spectrum (FHSS)
- Radio Controlled Torpedoes
- George Antheil & Self-playing Piano’s

Bluetooth Low Energy (BLE)	Point-to-Point Low energy consumption 2.4 – 2.485 GHz
Bluetooth Mesh	Many-to-Many Supports 32,767 nodes per mesh network

The Protocol

- Advertising
  - 3 Channels for advertisement 37, 38, 39
  - 4 Advertising PDU Types
- Connecting
  - 36 Channels (Japan, Spain, France have 23)
  - 1 MHz spacing
  - FHSS:
    - Channel = (currentChannel + hop) % 37

Link Layer Packet Organization



BLE 4.0/4.1

Preamble 1 byte	Access Address 4 bytes	Data Ch. PDU Header 2 bytes	Data Payload ≤ 27 bytes	Optional MIC 4 bytes	CRC 3 byte

L2CAP Header 4 bytes	ATT Header 3 bytes	ATT Data ≤ 20 bytes

BLE 4.2/5.0

Preamble 1 byte	Access Address 4 bytes	Data Ch. PDU Header 2 bytes	Data Payload ≤ 251 bytes	Optional MIC 4 bytes	CRC 3 byte

L2CAP Header 4 bytes	ATT Header 3 bytes	ATT Data ≤ 244 bytes

Broadcasting and Connections

- One way
- Connectionless
- Two Roles
  - Broadcaster
  - Observer
- iBeacons

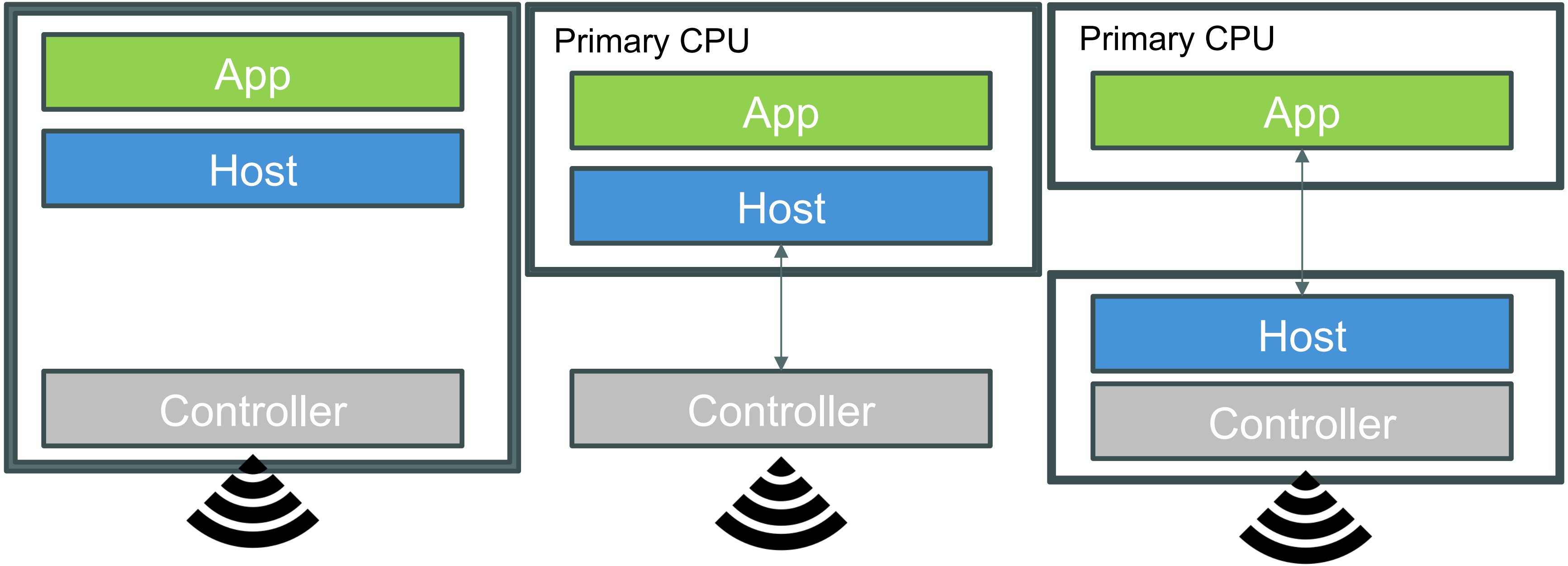
- Two way
- Additional Protocol Layers
- Two Roles
  - Central
  - Peripheral
- Phone to Thingy52

Connections

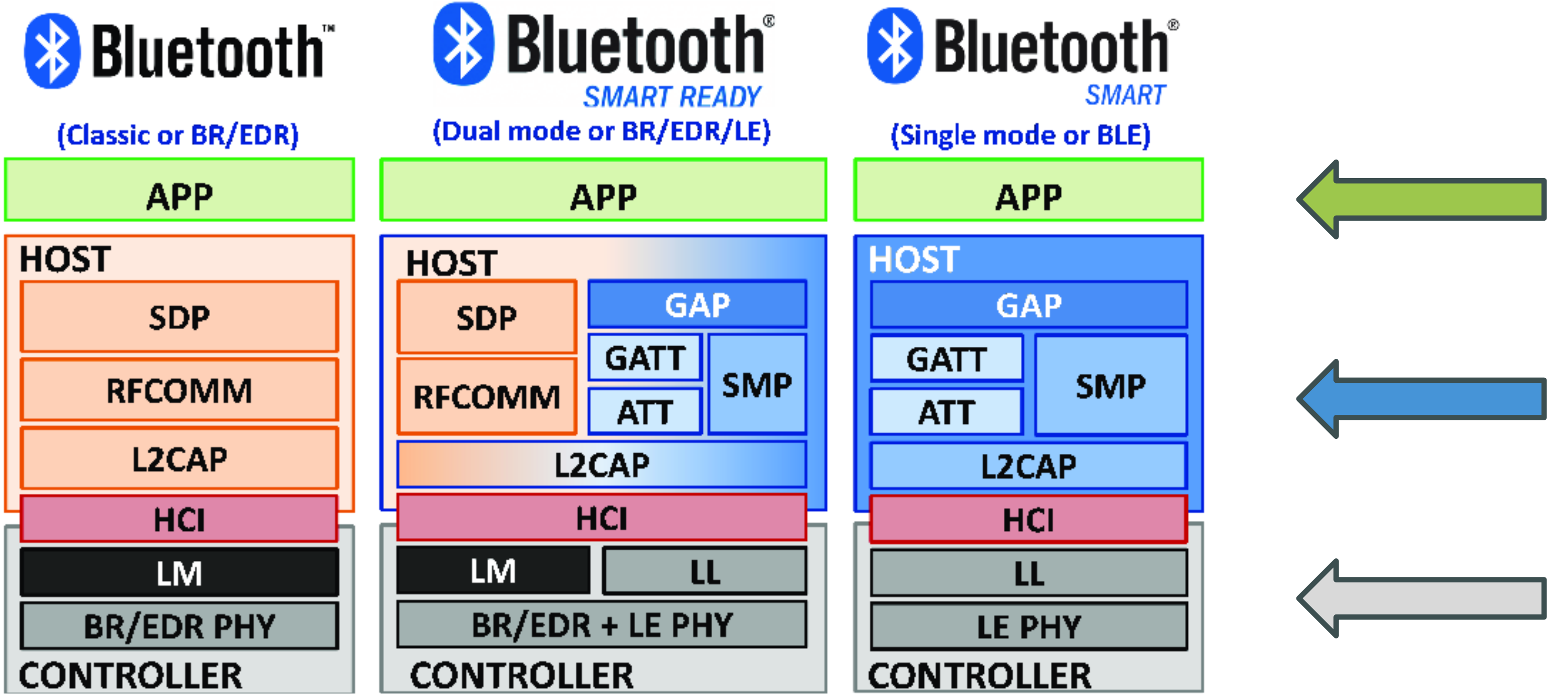
- Devices:
  - Central (i.e. Phone)
    - Connection Initiator
    - Controls timing and data exchange
  - Peripheral (i.e. Thingy 52)
    - Advertises
    - Accepts incoming connections

Common Configurations

- SoC
- IC over HCI
- Dual IC



Bluetooth Protocol Stack



Layers of Interest

- Logical Link
  - Modifies connection params
  - Performs encryption/ decryption

- HCI
  - Commands and Events for host and controller interaction

- L2CAP
  - ‘Like’ TCP
  - Enables many protocols coexisting
  - Encapsulation from upper to lower layers

Link Layer

- CRC creation and verification
- Encryption (AES)
- Random number generation

L2CAP

- Controls ATT and SM
- Fragments packets into 27 (4.1) / 251 (4.2+) byte payload

SM

- Protocol
- Security Key generation and exchange algorithms
- Pairing
- Bonding
- Encryption Reestablishment

Part II

IOActive®

Bluetooth Vulnerabilities

- Blueborne – Smart Devices, wormable via BLE
- Bleedingbit – Wireless APs, security bypass & malicious OTA
- SweynTooth – BLE chips, DoS

Bleedingbit

- https://www.armis.com/bleedingbit/

- Armis
- CVE-2018-16986
- CVE-2018-7080
- TI BLE Chip RCE Vulnerability
- Cisco, Aruba, Meraki

SweynTooth

- https://asset-group.github.io/disclosures/sweyntooth/
- 2019 / 2020
- Singapore University of Technology and Design
  - Matheus E. Garbelini, Sudipta Chattopadhyay, Chundong Wang

CVE-2019-16336 / CVE-2019-17519

- Cypress PSoC4/6 BLE Component 3.41/2.60
- *NXP KW41Z 3.40* SDK

- Link Layer Length Overflow
- DoS
- Potential for Further RCE

Part III

BLE Fuzzing

- A shift in research

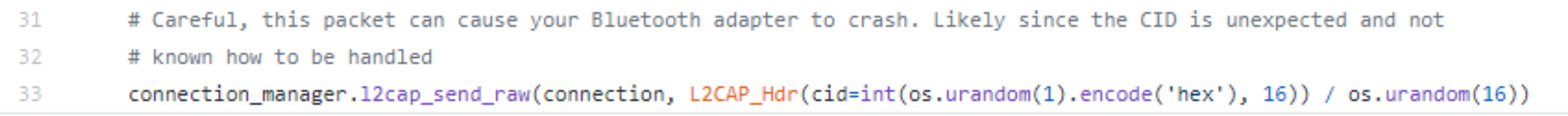
NCCGroup’s BLEsuite

- https://github.com/nccgroup/BLESuite

- BLE python library
- Fuzzing tool

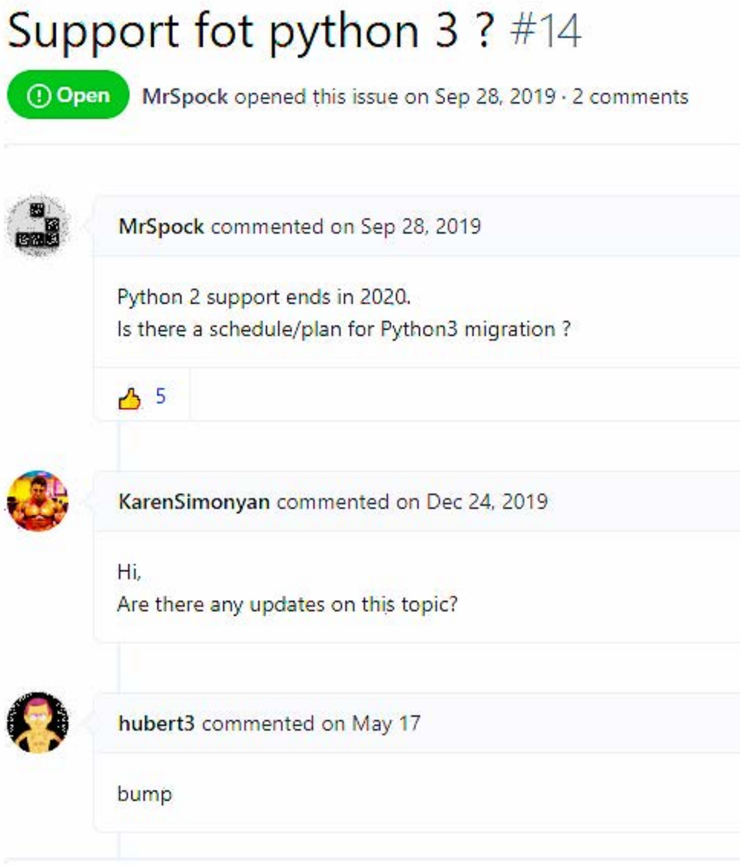
Foreshadowing

- https://github.com/nccgroup/BLESuite/blob/master/docs/examples/advanced_manual_packets.py
- Channel ID -



```
# Careful, this packet can cause your Bluetooth adapter to crash. Likely since the CID is unexpected and not
# known how to be handled
connection_manager.l2cap_send_raw(connection, L2CAP_Hdr(cid=int(os.urandom(1).encode('hex'), 16)) / os.urandom(16))
```

The Issues



Support fot python 3 ? #14

Open MrSpock opened this issue on Sep 28, 2019 · 2 comments

MrSpock commented on Sep 28, 2019

Python 2 support ends in 2020.
Is there a schedule/plan for Python3 migration ?

👍 5

KarenSimonyan commented on Dec 24, 2019

Hi,
Are there any updates on this topic?

hubert3 commented on May 17

bump

GO!

- https://github.com/go-ble/ble
- Go Module for BLE

Go BLE Scanner Demo

DEMO

Additional Info

- ‘Introduction to BLE Exploitation’ – IOActive webinar (May 2020) https://act-on.ioactive.com/acton/media/34793/ioactive-webinars#block-b1574346531854
- Getting Started With Bluetooth Low Energy: Tools and Techniques for Low-Power Networking
- Hacking Exposed Wireless: Wireless Security Secrets and Solutions

https://www.youtube.com/playlist?list=PLkMJSkfvo46OWMWzCqQUkFdVg27ILF7Hi

Thank You

IOActive®

IOActive Presentation Content

Legal Notices

- **Disclaimer Notification**
  The views, opinions, findings, conclusions, positions, and/or recommendations expressed herein are those of the authors individually and do not necessarily reflect the views, opinions, or positions of IOActive, Inc.
- **No Warranties or Representations**
  The information presented herein is provided "AS IS" and IOActive disclaims all warranties whatsoever, whether express or implied. Further, IOActive does not endorse, guarantee, or approve, and assumes no responsibility for nor makes any representations regarding the content, accuracy, reliability, timeliness, or completeness of the information presented. Users of the information contained herein assume all liability from such use.
- **Publicly Available Material**
  All source material referenced in this presentation was obtained from the Internet without restriction on use.
- **Fair Use**
  This primary purpose of this presentation is to educate and inform. It may contain copyrighted material, the use of which has not always been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of cyber safety and security. This material is distributed without profit for the purposes of criticism, comment, news reporting, teaching, scholarship, education, and research, and constitutes fair use as provided for in section 107 of the Copyright Act of 1976.
- **Trademarks**
  IOActive, the IOActive logo and the hackBOT logo are trademarks and/or registered trademarks of IOActive, Inc. in the United States and other countries. All other trademarks, product names, logos, and brands are the property of their respective owners and are used for identification purposes only.
- **No Endorsement or Commercial Relationship**
  The use or mention of a company, product or brand herein does not imply any endorsement by IOActive of that company, product, or brand, nor does it imply any endorsement by such company, product manufacturer, or brand owner of IOActive. Further, the use or mention of a company, product, or brand herein does not imply that any commercial relationship has existed, currently exists, or will exist between IOActive and such company, product manufacturer, or brand owner.
- **Copyright**
  ©2020 IOActive, Inc. All rights reserved. This work is protected by US and international copyright laws. Reproduction, distribution, or transmission of any part of this work in any form or by any means is strictly prohibited without the prior written permission of the publisher.