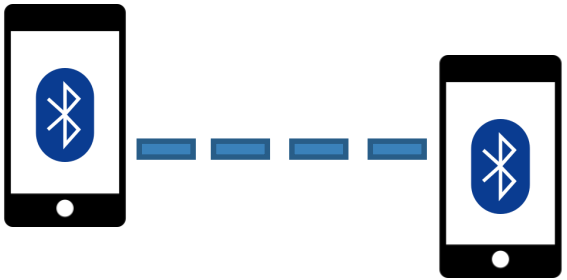
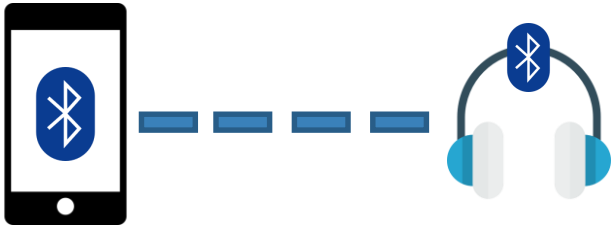
Bluetooth

Vulnerability

Bluetooth ???

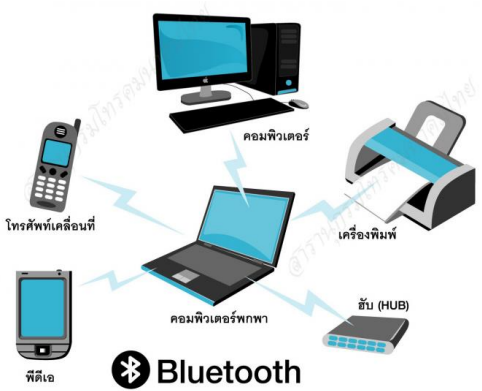
คือ เทคโนโลยีในการรับส่งข้อมูลระหว่าง Device 2 ตัว





Bluetooth

Bluetooth จะใช้สัญญาณวิทยุความถี่สูง 2.4 GHz. ซึ่งแต่ละประเทศความถี่นั้นจะต่างกันไป อย่างในแถบยุโรปและอเมริกา จะใช้ช่วง 2.400 ถึง 2.4835 GHz. แบ่งออกเป็น 79 ช่องสัญญาณ และจะใช้ช่องสัญญาณที่แบ่งนี้ เพื่อส่งข้อมูลสลับช่องไปมา 1,600 ครั้งต่อ 1 วินาที ส่วนที่ญี่ปุ่นจะใช้ความถี่ 2.402 ถึง 2.480 GHz. แบ่งออกเป็น 23 ช่อง ระยะทำการของ Bluetooth จะอยู่ที่ 5-10 เมตร



การพัฒนาของ BLUETOOTH

1.0

Version 1.0 และ1.0B - 1.1-1.2

Device address (BD-ADDR) ในการส่งข้อมูลผ่านการ Connecting (การส่งข้อมูลแบบนี้ยังมีปัญหาอยู่)

2.0

Version 2.0+EDR

เพิ่ม Enhanced Data Rate(EDR) เพื่อให้การเคลื่อนย้ายข้อมูลทำได้เร็วขึ้น อัตราความเร็วของ EDR อยู่ 3 เมกกะบิตต่อวินาที

3.0

Version 3.0 + HS

เวอร์ชั่นนี้ถูกปรับปรุงโดย Bluetooth SIGมีการรองรับการขนส่งข้อมูลด้วยความเร็วสูงสุด 24 เมกกะบิตต่อวินาที

4.0

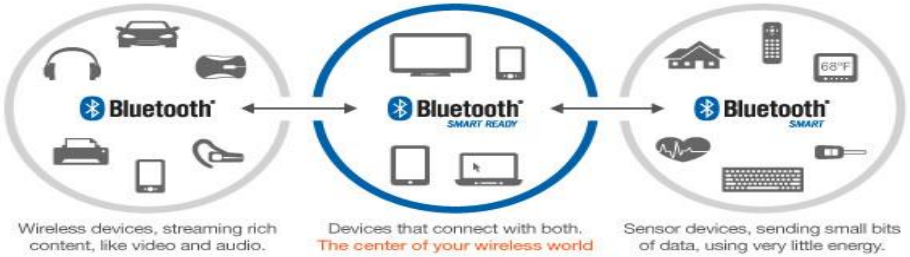
Version V4.0 - 4.2

Protocols ที่ใช้พลังงานต่ำและนำเทคโนโลยี ultra-low power Bluetoothเข้ามาใช้ ยกตัวอย่างกรณีที่มีการใช้เทคโนโลยีนี้ เช่น การแสดงแสดงหมายเลขผู้โทรศัพท์

BLUETOOTH

BLUETOOTH 2.0, 3.0, 4.0,มีการเปลี่ยนแปลในระดับ HARDWARE

BLUETOOTH 4.0, 4.1, 4.2,มีการเปลี่ยนแปลในระดับ FEATURE



EDR กับ HS เหมือนกัน
คือมีการเพิ่มความเร็วรับส่งข้อมูล

HS = HIGSSPEED
EDR = ENHANCED SATA RATES

เทคโนโลยีBluetooth นี้ก็ได้ถูกพัฒนามาจนเป็น “Bluetooth 5” ซึ่งว่ากันว่าทรงประสิทธิภาพมากที่สุดเท่าที่เคยมีเทคโนโลยีนี้มา อีกทั้งหลักใหญ่ใจความของมันยังให้ความสำคัญเน้นหนักไปที่เรื่องของ Internet of Things (IoT), สมาร์ทโฮม (Smart Home) และการฟังเพลงแบบไร้สาย (Wireless Audio)

BLUETOOTH 5.0

BLUETOOTH 5.0

5 มีแบนด์วิดธ์สูงสุดที่ 2Mbps ในทางปฏิบัติหมายความว่ามันเร็วพอและไว้ใจได้มากพอที่จะใช้ระบบไร้สายทำการอัปเดทเฟิร์มแวร์หรือใช้อัปโหลดข้อมูลสำคัญ Bluetooth

สามารถรับ-ส่งข้อมูลได้เร็วกว่า Bluetooth 4.2 LE (Low Energy) ถึง 2 เท่า เชื่อมต่อได้ในระยะห่างไกลกว่าถึง 4 เท่า และสามารถส่งผ่านปริมาณข้อมูลในหนึ่งช่วงเวลาได้มากกว่าถึง 8 เท่ามีระยะห่างในการเชื่อมต่อระหว่างอุปกรณ์เพิ่มขึ้นเป็น 800 ฟุต (ประมาณ 240 เมตร)

ข้อดีและข้อเสียBLUETOOTH

ข้อดี

1.เพิ่มความสะดวกสบายในการใช้อุปกรณ์อิเล็คโทรนิคต่างๆ
2. สามารถโอนถ่ายข้อมูลต่างๆได้ง่ายและรวดเร็วขึ้น
3. ประหยัดค่าใช้จ่ายในการส่งข้อมูลหรือรูปภาพต่างๆ
4. การใช้บูลทูธจะช่วยประหยัดเวลาในการตั้งอุปกรณ์ต่างๆ และสามารถเคลื่อนย้ายอุปกรณ์ได้ง่าย
5. ลดความกังวลในการใช้โทรศัพท์ เนื่องจากถ้าผู้ใช้เลือกใช้ Smalltalk แบบมีสายต่อก็ต้องคอยกังวลว่า
6. เมื่อเปรียบเทียบกับการใช้อินฟาเรดแล้ว การใช้ Bluetooth มีข้อดีกว่า เนื่องจากการรับส่งข้อมูลแบบอินฟาเรดต้องใช้แสงเป็นสื่อในการติดต่อและผู้ส่งกับผู้รับ

ข้อเสีย

1.ความง่ายดายในการโอนถ่ายข้อมูลอาจทำให้เกิดอาชญากรรมเพิ่มมากขึ้นได้ถ้าบุคคลเหล่านั้นนำ
บูลทูธไปใช้งานในแบบที่ไม่เหมาะสม
2. ถ้ามีการเปิดบูลทูธทิ้งไว้นานอาจมีกลุ่มบุคคลที่ไม่ประสงค์ดีปล่อยตัวไวรัสมาที่อุปกรณ์อิเล็คโทรนิคของ
เราได้ ซึ่งก่อให้เกิดความเสียหายต่อทรัพย์สินและข้อมูลต่างๆได้
3. การใช้ Booth Headset และโทรศัพท์มือถืออย่างเพลิดเพลินและความสะดวกสบาย อาจทำให้ผู้ใช้ขาดความระมัดระวังได้
4. การส่งข้อมูลทาง Bluetooth อาจทำให้เกิดการดักฟังหรือการลักลอบขโมยข้อมูลต่างๆได้ถึงแม้ว่าจะทำได้ยากก็ตาม

Bluetooth Vulnerability

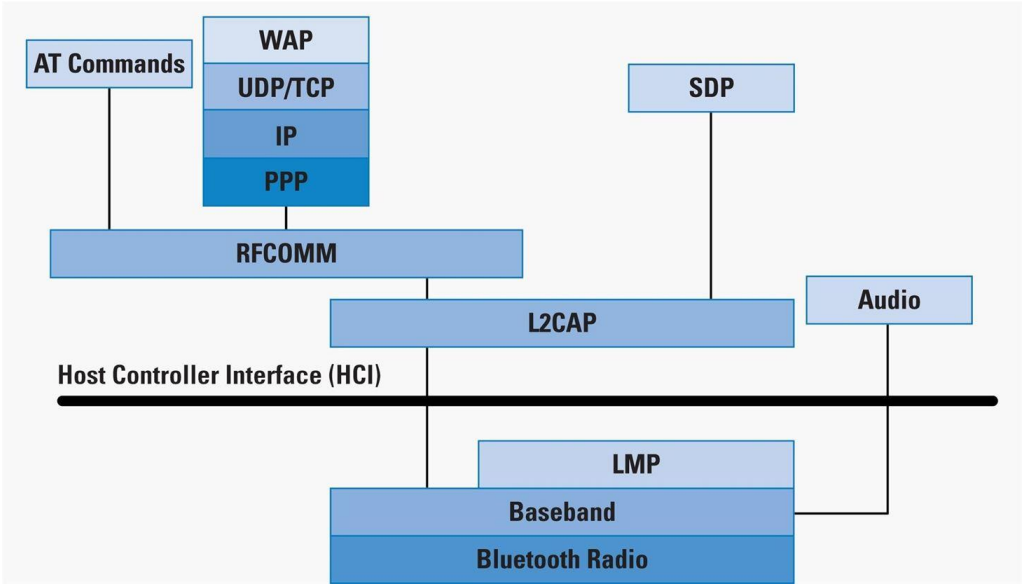
Bluetooth

มีความเสี่ยงของการถูก
โจรกรรมทางข้อมูล

ช่องโหว่ของบลูทูธ

1.ไม่มีการรักษาความปลอดภัยที่ใช้งานอยู่
2.ความปลอดภัยระดับบริการ ผู้จัดการความปลอดภัยส่วนกลางจัดการการรับรองความถูกต้องการกำหนดค่าและการอนุญาต อาจไม่สามารถเปิดใช้งานโดยผู้ใช้ ไม่มีความปลอดภัยระดับอุปกรณ์
3. ความปลอดภัยระดับอุปกรณ์ การรับรองความถูกต้องและการเข้ารหัสตามคีย์ลับ เปิดเสมอ บังคับใช้การรักษาความปลอดภัยสำหรับการเชื่อมต่อระดับต่ำ

- Bluetooth Core Protocols
Baseband: LMP, L2CAP, SDP
- Cable Replacement Protocol: RFCOMM
-Telephony Control Protocol: TCS Binary, AT-commands
- Adopted Protocols: PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE



Bluetooth Protocol Stack

BlueBorne™

เตือนภัยช่องโหว่ชื่อ BlueBorne (บลูบอร์น) อาจจะถูกขโมยข้อมูล หรือถูกติดตั้งมัลแวร์ที่เปิดใช้งานบลูทูธ (Bluetooth) และอยู่ในรัศมีประมาณ 10 เมตร โดยที่ตัวอุปกรณ์ไม่จำเป็นต้องจับคู่ (Pair) กับอุปกรณ์ที่ใช้โจมตี รวมถึงไม่จำเป็นต้องเปิดโหมดค้นหาอุปกรณ์ (Discovery mode) แต่อย่างใด

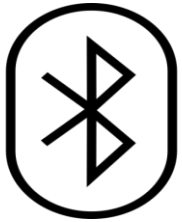
BlueBorne ส่งผลกระทบต่ออุปกรณ์บลูทูธทั่วโลก ไม่ว่าจะเป็นระบบปฏิบัติการ Android, Apple iOS, Microsoft หรือ Linux ตั้งแต่สมาร์ทโฟน แท็บเล็ต โน๊ตบุ๊ค อุปกรณ์ IoT ไปจนถึงรถยนต์อัจฉริยะรวมแล้วกว่า 5,300 ล้านเครื่อง

Bluetooth Vulnerability

Kali คือระบบปฏิบัติการณ์ลินุกซ์ (Linux) ตัวนึงของคอมพิวเตอร์ เหมือนกับการที่มือถือเรามี iOS กับ Android คอมฯ เราก็มีระบบปฏิบัติการณ์หลายตัวอย่าง MacOS, Windows และลินุกซ์ ซึ่งโดยปกติแล้วลินุกซ์มักจะถูกใช้ใน เครื่องเซิร์ฟเวอร์เช่นไว้รันเซิร์ฟเวอร์

แต่ Kali เป็นลินุกซ์ที่ออกแบบมาสำหรับ “งานด้านความปลอดภัยระบบไอที” โดยการที่ติดตั้งซอฟต์แวร์ต่าง ๆ ที่มักจะถูกใช้งานบ่อย ๆ ในการทำงานเอาไว้เรียบร้อยแล้ว หรือยังไม่ได้ติดตั้งแต่ว่า สามารถติดตั้งได้โดยง่าย ผ่านระบบติดตั้งโปรแกรมที่มีให้เรียกว่า software repository ของ Kali โดยเฉพาะ

ตัวอย่างของแถบเครื่องมือKali ในฟังก์ชั่นของBluetooth



เครื่องมือของKali

1.Bluelog: เครื่องมือสำรวจไซต์บลูทูธ มันสแกนพื้นที่เพื่อค้นหาอุปกรณ์ที่ค้นพบได้จำนวนมากในพื้นที่แล้ว บันทึกลงในไฟล์

2.Bluemaho: ชุดเครื่องมือที่ใช้ GUI สำหรับการทดสอบความปลอดภัยของอุปกรณ์ Bluetooth

3.Blueranger: สคริปต์ Python แบบง่ายที่ใช้ i2cap pings เพื่อค้นหาอุปกรณ์บลูทูธ และกำหนดระยะทางโดยประมาณ

4.Btscanner: เครื่องมือที่ใช้ GUI นี้สแกนหาอุปกรณ์ที่สามารถค้นพบได้ภายในระยะ

5.Redfang: เครื่องมือนี้ช่วยให้เราค้นหาอุปกรณ์บลูทูธ ที่ซ่อนอยู่

เครื่องมือของKali

6.Spooftooph: นี่คือเครื่องมือการปลอมแปลงบลูทูธ

7.Bluesnarfing: การโจมตีนี้ใช้ข้อมูลจากอุปกรณ์ที่ใช้เทคโนโลยี Bluetooth ซึ่งอาจรวมถึงข้อความ SMS ข้อมูลปฏิทินรูปภาพสมุดโทรศัพท์และการแชท

8.Bluebugging: ผู้โจมตีสามารถควบคุมโทรศัพท์ของเป้าหมายได้ Bloover ได้รับการพัฒนาเป็นเครื่องมือ POC สำหรับจุดประสงค์นี้

9.Bluejacking: ผู้โจมตีส่ง "นามบัตร" (ข้อความ) ซึ่งหากผู้ใช้อนุญาตให้เพิ่มในรายชื่อผู้ติดต่อผู้โจมตีสามารถส่งข้อความเพิ่มเติมได้

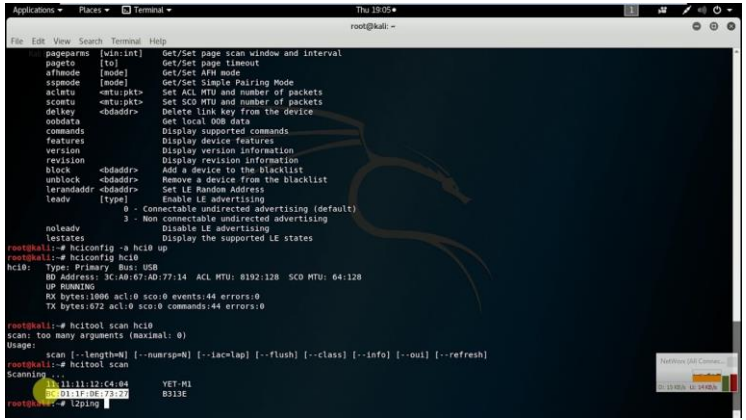
10.Bluesmack: การโจมตี DoS จากอุปกรณ์บลูทูธ

ตัวอย่างการใช้งาน(Kali)ในการแฮกบลูทูธ

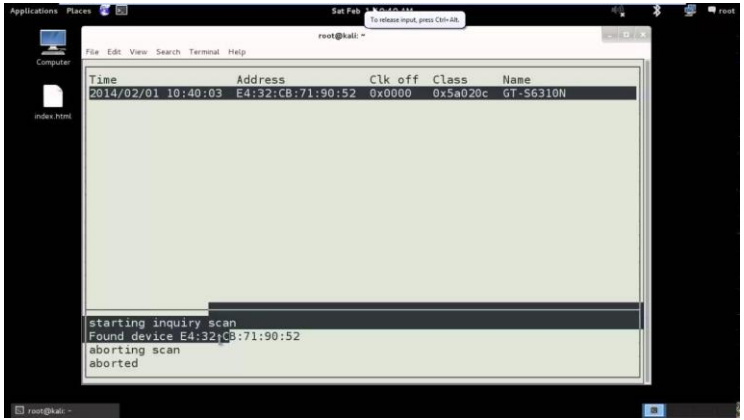
```
root@kali:~# hciconfig hci0 up
root@kali:~# hciconfig hci0
hci0:   Type: BR/EDR  Bus: USB
        BD Address: A0:02:DC:11:4F:85  ACL MTU: 310:10  SCO MTU: 64:8
        UP RUNNING PSCAN
        RX bytes:913 acl:0 sco:0 events:43 errors:0
        TX bytes:915 acl:0 sco:0 commands:43 errors:0
```

(การตั้งค่า)

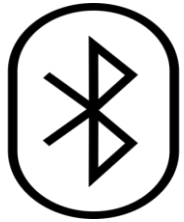
ตัวอย่างการใช้งาน(Kali)ในการแฮกบลูทูธ



การค้นหาสัญญาณบลูทูธเพื่อทำการเชื่อมต่อ เมื่อทำการเชื่อมต่อสำเร็จก็สามารถทำการโจรกรรมข้อมูลหรือปล่อยมัลแวร์ทำลายโทรศัพท์ของเป้าหมายได้



***หมายเหตุบลูทูธตั้งแต่4.0+ขึ้นไปมีระบบป้องกันการโจรกรรมข้อมูลทำให้เกอดการเชื่อมต่อได้ยาก



ขอบคุณครับ