AppSec Labs Ltd.
info@appsec-labs.com
https://appsec-labs.com

Hacking Bluetooth Low Energy Based Applications

Tal Melamed
Application Security Expert
Tal@appsec.it

The Twelfth International Conference on Internet Monitoring and Protection
ICIMP 2017
June 25 - 29, 2017- Venice, Italy

Discussed Topics

- Key aspects in Bluetooth Low Energy (BLE)
- How is it different than Bluetooth Classic?
- Where is the risk?
- Bluetooth Low Energy Architecture
- The Security Manager
- Bluetooth Pairing
- Generic Attribute Profile (GATT)
- Man-in-the-Middle (MitM)
- Related work
- Possible Mitigations
- Bibliography

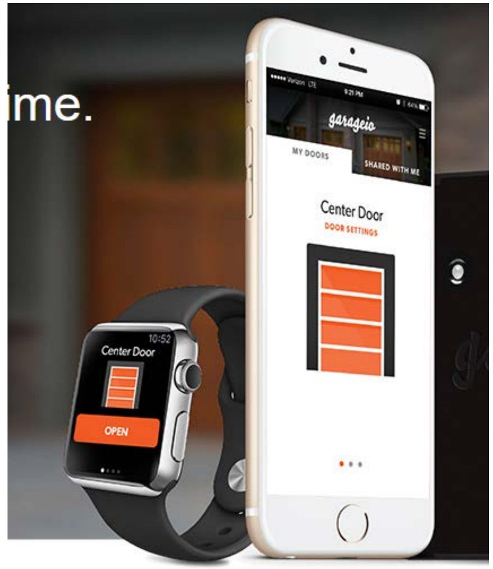
What is Bluetooth Low Energy

- Bluetooth Low Energy (BLE)
  - a.k.a Bluetooth Smart, part of Bluetooth 4
- Designed to be power-efficient
- Significantly smaller and cheaper.
- Low cost and ease of implementation lead BLE to be widely used among IoT devices and applications
- Wearables, sensors, lightbulbs, medical devices, and many other smart-products.
- 48 billion IoT devices expected by 2021, and Bluetooth—predicted to be in nearly one-third of those devices

Where is the difference?

- BLE vs BT Classic
  - Different architecture (Master-Slave)
  - Different modulation parameters
  - Different channels
  - Different channel-hopping scheme
  - Different packet format
  - Different packet whitening

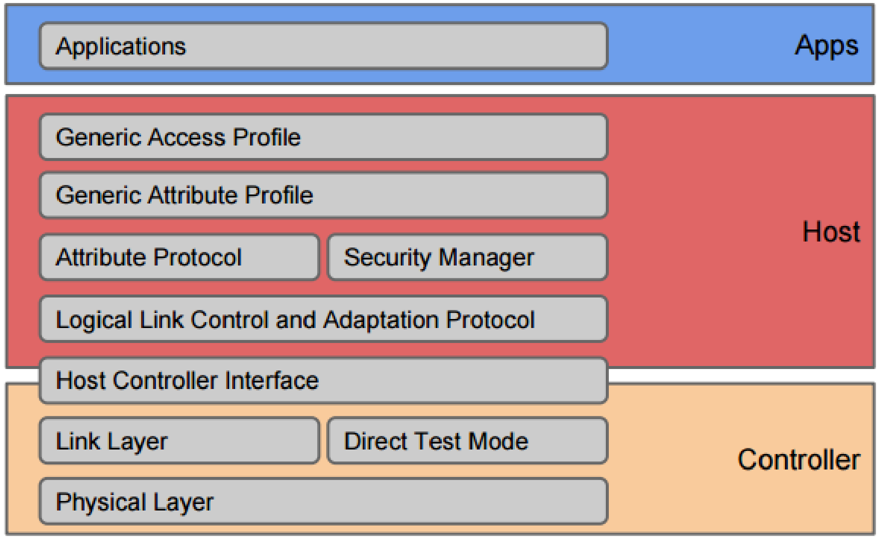
Where is the risk?



- BLE products can be found in our day-to-day life…

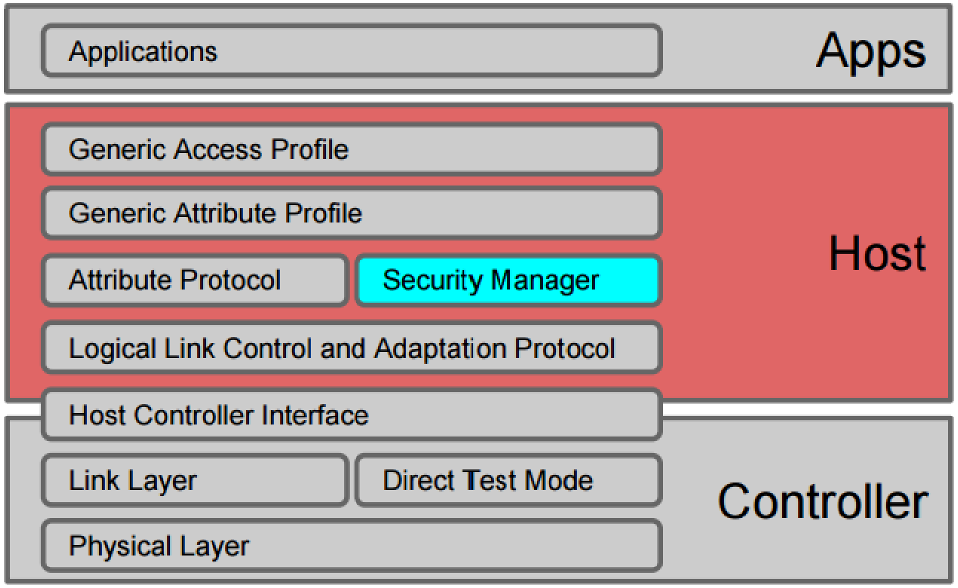
BLE Architecture

- Apps
  - Applications are built on top
  - Interacts with host layer only
  - Different API's depending on the application environment
- Host
  - Sits on top of the Radio
  - Provides API to application
- Controller
  - Radio Control
  - Connection Linking
  - Radio Testing
  - Interface to Host



Security Manager

- Three phase process on connection
  - Pairing feature exchange
  - Short term key generation
  - Transport specific key distribution
- Implements a number of cryptographic functions

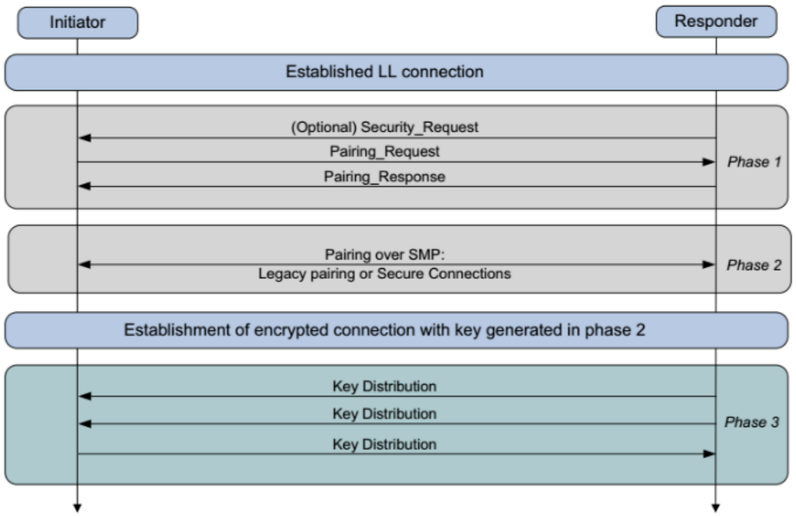


Security Manager

- Has AES-128 capabilities
- Uses Key Distribution to share various keys
  - Bluetooth Smart (4.0) uses an insecure
  - BLE 4.1/5.0 uses EC-DH for key exchange
- Pairing encrypts the link using a Temporary Key (TK)
  - Derived from passkey
  - Then distribute keys

Pairing

- Using keys to encrypt the communication
  - The keys can be used to encrypt future reconnections
- Can also verify signed data, or perform random address resolution



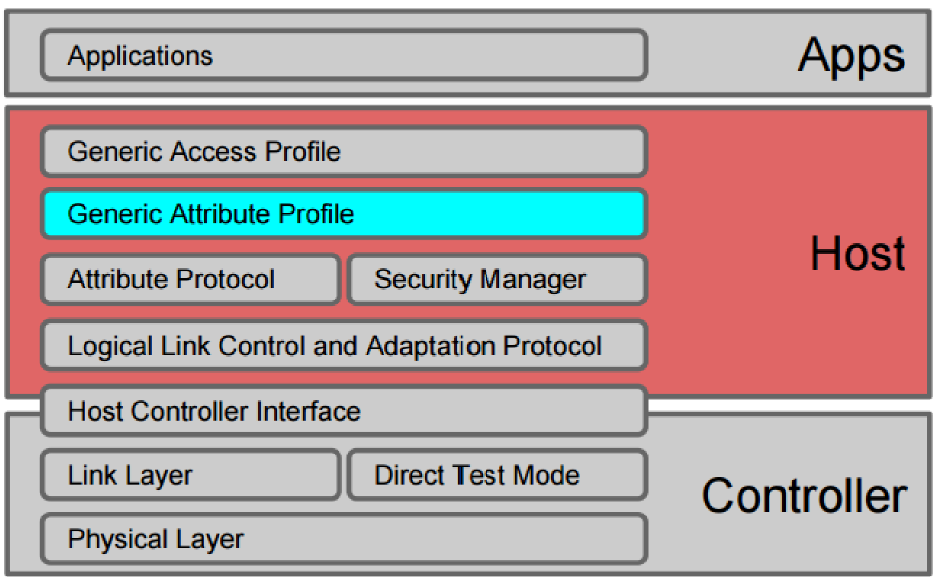
- 3-phase for pairing
  - Pairing Feature Exchange
  - Short Term Key (STK) Generation (legacy pairing)
    - Long Term Key (LTK) Generation (4.1/5.0 Secure Connections)
  - Transport Specific Key Distribution

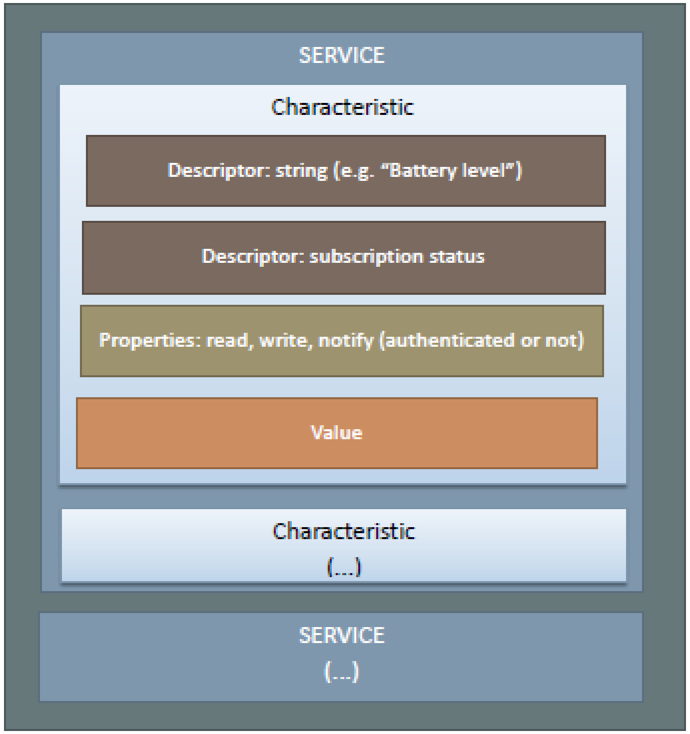
Pairing

- How to determine the temporary key (TK)?
  - **JustWorks™**
    - Legacy, most common
    - Devices without display cannot implement other
    - Its actually a key of zero, that's why it just works...
  - **6-digit PIN**
    - In case the device has a display
    - 1 million options (BF-able)
  - **Out of band (OOB)**
    - Does not share secret key over the 2.4 GHz band (used by protocol)
    - Makes use of other mediums (e.g. NFC)
    - Once secret keys are exchanged, encrypts the channel
    - Not common, barely used

Generic Attribute Profile (GATT)

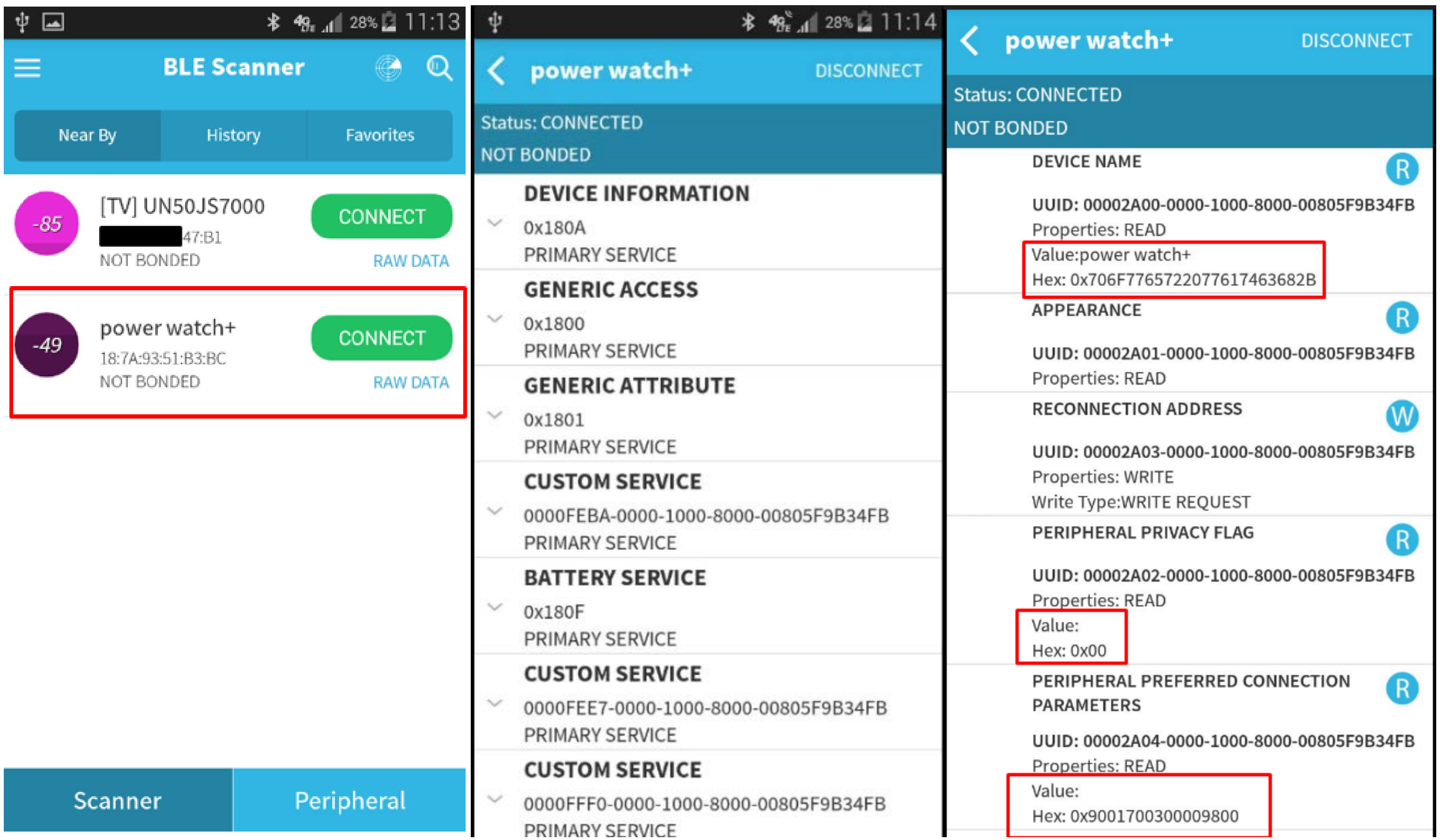
- Services & characteristic are identified by an associated UUID
- A characteristic contains a single value ("attribute")
  - Can be read, written to or subscribed for notifications



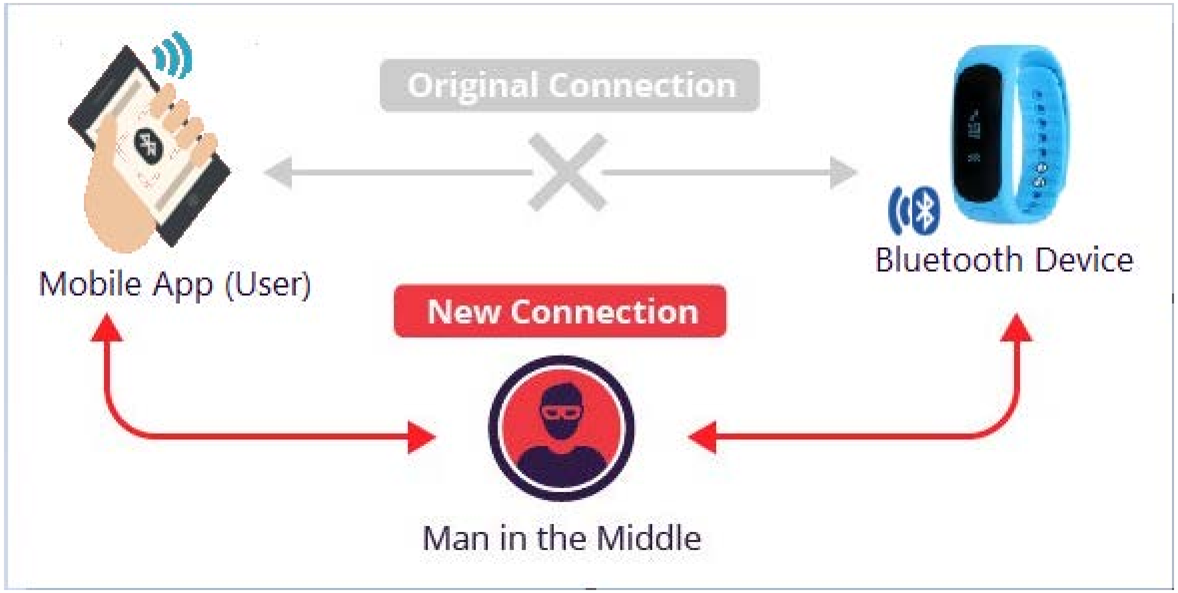


Discovering Services - Example

- Any BLE scanner app, downloaded from the store, can read data from and write data to the smart-device

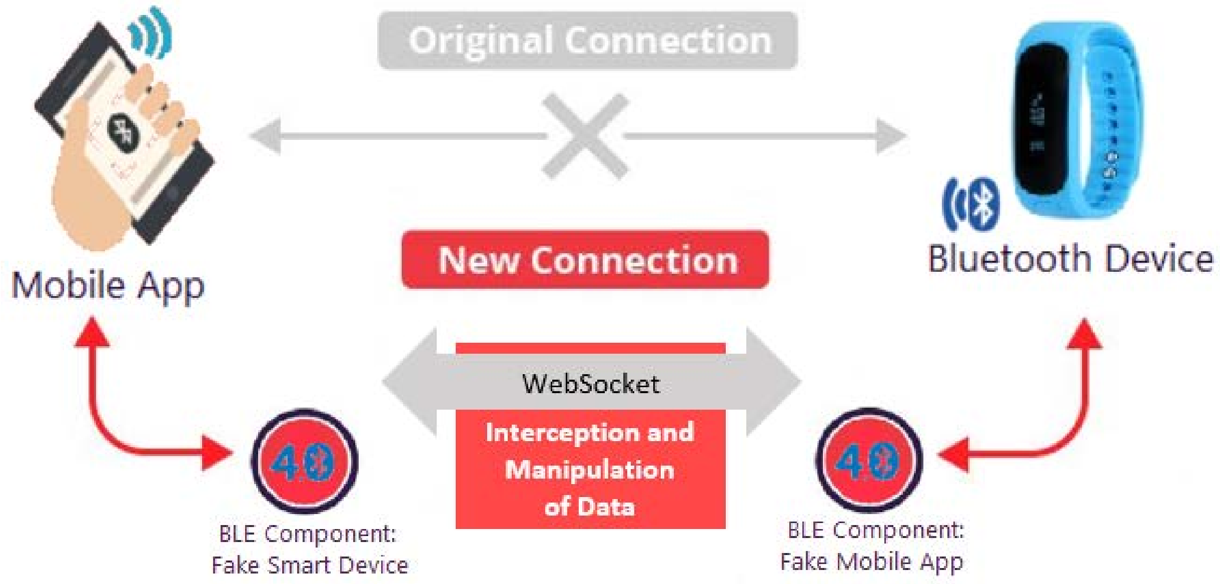


Normal Man-in-the-Middle (MitM)



- Why normal MitM won't work?
  - A BLE adapter cannot serve as both ends
  - One will have to serve as the client (app)
  - Another as the server (ble device)

BLE Man-in-the-Middle (MitM)

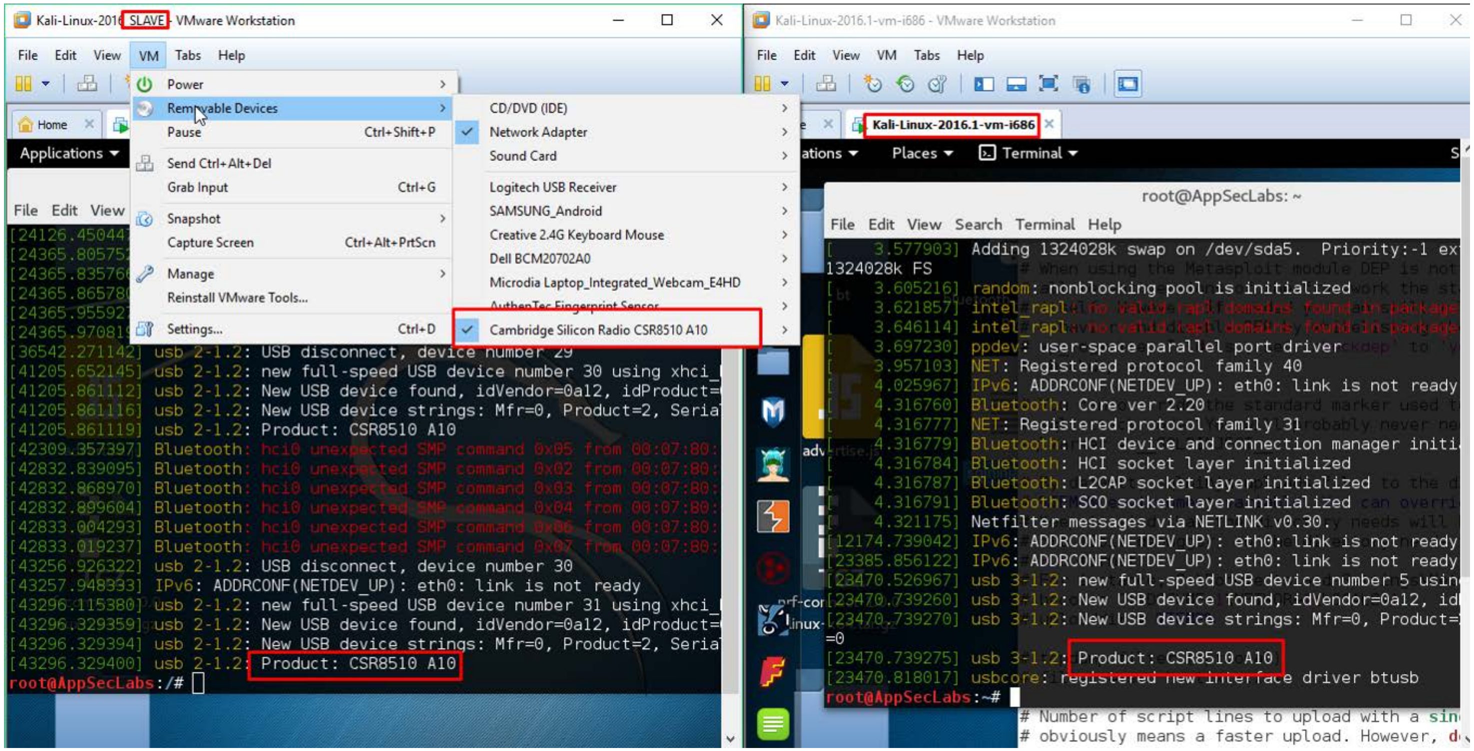


- After each BLE-adapter (component) is connected to the designated device – they communicate with each other over WebSocket
- Which gives them the ability to serve as MitM

What to we need for MitM

- CSR 4.0 dongle x2
  - Works as Slave/Master

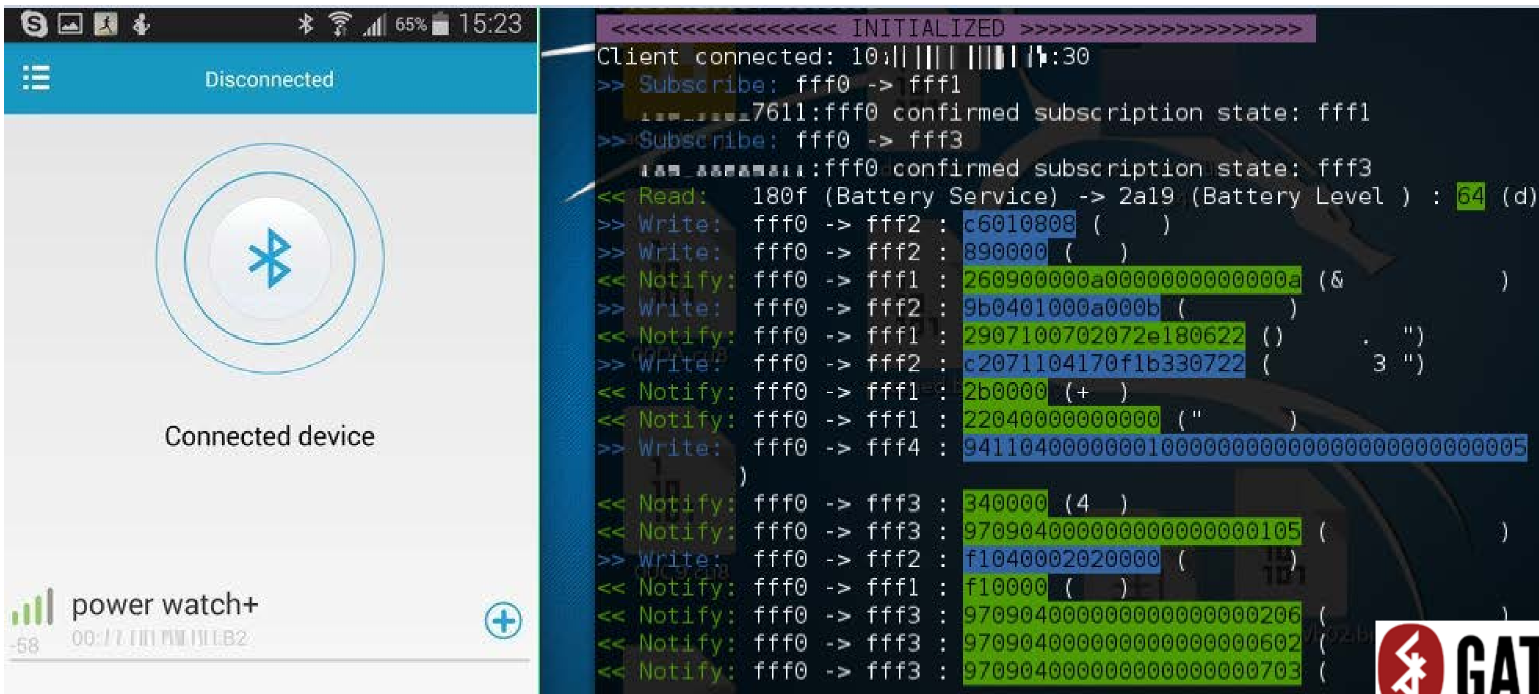
- Download Kali-linux VM and Clone



GATTacker

- BLE (Bluetooth Low Energy) security assessment using Man-in-the-Middle

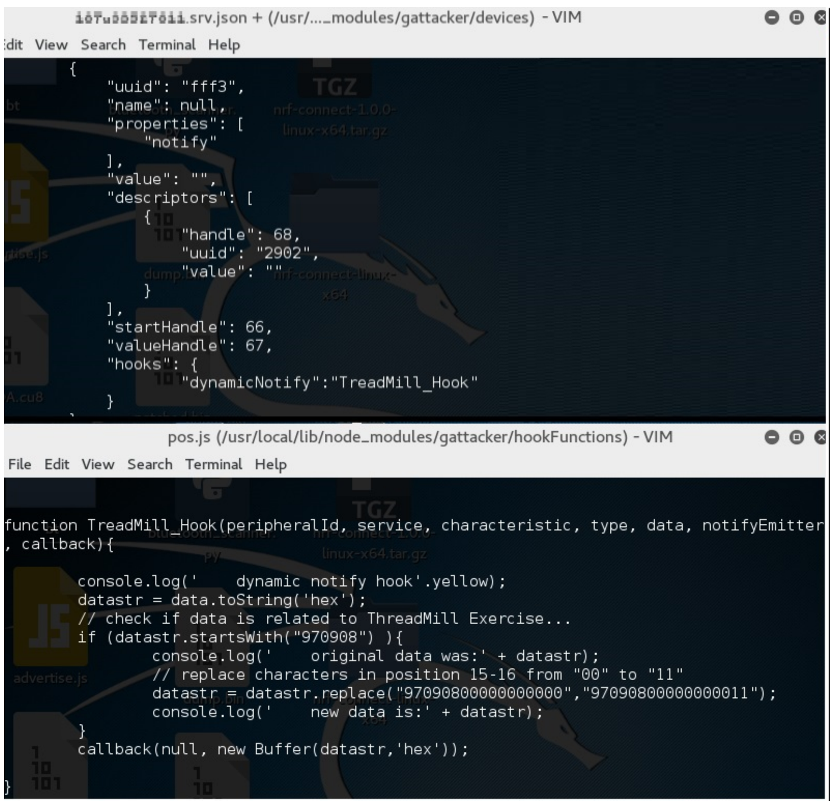
https://github.com/securing/gattacker

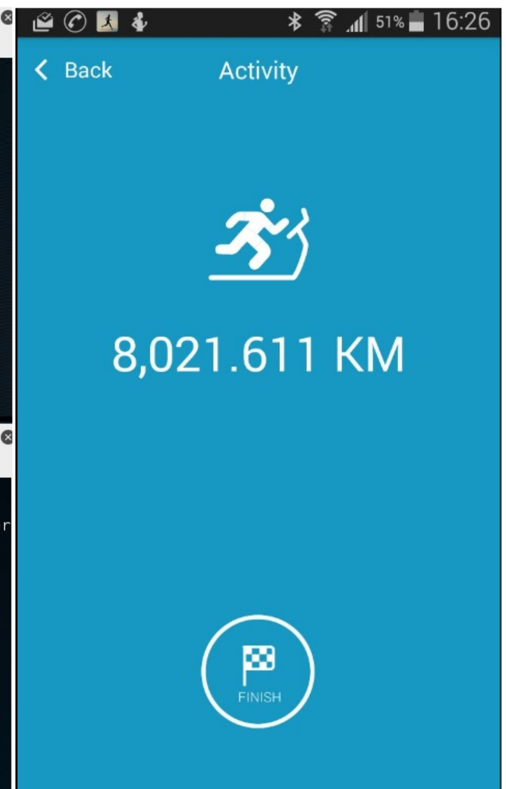


GATTack.io
OUTSMART THE THINGS

Hooking events using GATTacker

- Hooking into smart-watch sports counter and modifying the data (kilometrage) sent from the smart watch into the device





BtleJuice

- Bluetooth Smart (LE) Man-in-the-Middle framework

https://github.com/DigitalSecurity/BtleJuice

BtleJuice

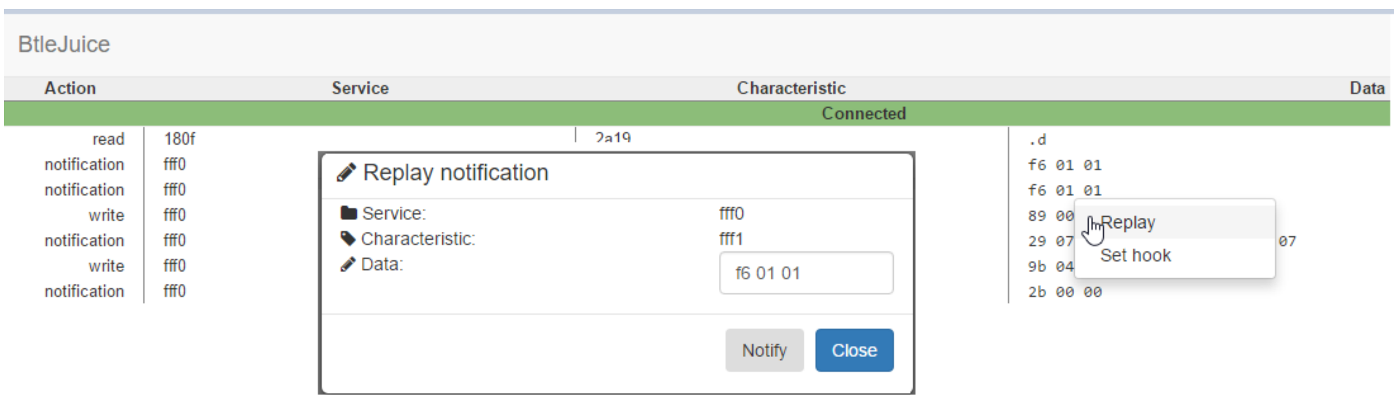
Action	Service	Characteristic	Data
Connected			
read	180f	2a19	.d
write	fff0	fff2	c6 01 08 08
write	fff0	fff2	89 00 00
notification	fff0	fff1	26 09 00 00 7b 00 00 02 00 00 00 .y
notification	fff0	fff1	29 07 11 04 17 10 .4 0e 00 28
write	fff0	fff2	89 00 00
notification	fff0	fff1	29 07 11 04 17 10 .4 14 00 .2
write	fff0	fff2	89 00 00
notification	fff0	fff1	29 07 11 04 17 10 .4 1a 00 .<
write	fff0	fff2	89 00 00
notification	fff0	fff1	29 07 11 04 17 10 .4 21 00 07
write	fff0	fff2	89 00 00
notification	fff0	fff1	29 07 11 04 17 10 .4 27 00 01
write	fff0	fff2	89 00 00
notification	fff0	fff1	29 07 11 04 17 10 .4 2d 00 0b
write	fff0	fff2	89 00 00

- Replay & on-the-fly data modification
- Web interface

Replay Attack using BtleJuice

- Remote control over the victim's mobile using *Replay Attack*

  - *Taking pictures*
  - *Playing music*



Possible attacks and countermeasures

- Attacks on advertisements
  - The attacker clones the advertisement and broadcasts the fake device
  - The device will try to connect and fail
  - **Countermeasures**:
    - Do not rely on received packets for critical functionality

- Attacks on exposed services
  - If the device offers services possible to access without authentication, an attacker can:
    - Brute-force data (e.g. guessing the password)
    - Fuzzing (Sending improper values to characteristics)
    - Logic vulnerabilities
  - **Countermeasures:**
    - Restrict access to services (e.g. least privilege)
    - Perform input validation
    - Time-limited provisioning (expose services only for a limited time after power-up, or dedicated button)

Attacks on Pairing

- An attacker can trick the user into re-initiation of the pairing using Jamming, cloning, etc.
- **Countermeasures:**
  - "Something you have" (e.g. allow pairing initiation only after performing the required action on the smart device - e.g. push a dedicated button)
  - Mobile app should warn when wrong MAC is used.

Man-in-the-Middle (MitM) attack

- Unencrypted transmission can be intercepted via passive eavesdropper
  - Exposing sensitive data (health data, passwords, etc.)
  - Data can be tampered with
  - Replay attack (e.g. unlock device)
- **Countermeasures:**
  - Encrypt data in transit, sign it and validate the input

Summary

- This poster confirms that BLE is insecure and vulnerable against passive eavesdropping.
- In particular, I have shown that a passive eavesdropping can easily become an active MitM attack that enables a possible hacker not only to listen to the communication, but also to intercept and manipulate the data.
- By performing a MitM attack, hackers can even control from remote the mobile device used to communicate with the Bluetooth smart device.
- With the release of the Bluetooth Core Specification version 4.2, BLE Security has been significantly improved by the new LE Secure Connections pairing model
- Additional security and privacy related features are added in the Bluetooth Core Specification v5, recently released by Bluetooth.
- It is vital to be aware and fully understand the limitations of the smart devices that we use rather than blindly relying on them.
- It is essential to implement security protections on the application-side to protect against malicious activity, by implementing additional security controls, such as data encryption, strong authentication and authorization mechanisms, and other security best practices.

Short Bibliography

- Bluetooth, S.I.G, SIG introduces Bluetooth Low Energy wireless technology, the next generation of Bluetooth wireless technology, *press release*, 2009.
- Ryan, Mike. Bluetooth: With Low Energy Comes Low Security, *WOOT*, 2013. Online, https://www.usenix.org/system/files/conference/woot13/woot13-ryan.pdf. Accessed on: 30 Apr. 2017.
- Bluetooth S.I.G., Proprietary Information Security, Bluetooth Low Energy. Online, https://www.bluetooth.com/~/media/files/specification/bluetooth-low-energy-security.ashx. Accessed on: 30 Apr. 2017.
- Bluetooth Specifications. Online, https://www.bluetooth.com/specifications. Accessed on: 30 Apr. 2017.
- Jasek S., GATTacking Bluetooth Smart devices, BlackHat USA 2016. Online, http://gattack.io/whitepaper.pdf. Access on: 30 Apr 2017.
- Cauquil D., BtleJuice: the Bluetooth Smart MitM Framework, DEF CON 24 Internet of Things Village, 2016. Video Online, https://www.youtube.com/watch?v=lcn07TclnS0. Accessed on: 30 Apr. 2017.
- Melamed T., R U aBLE? BLE Application Hacking, *OWASP*, 2017. Online, http://sl.owasp.org/melamed17. Accessed on: 30 Apr. 2017.