Wi-attack: Cross-technology Impersonation Attack against iBeacon Services

Xin Na, Xiuzhen Guo, Yuan He, Rui Xi

School of Software & BNRist, Tsinghua University
Bluetooth Low Energy

Traditional Bluetooth Devices
Streaming rich content

Bluetooth Ready Devices

BLE Devices
Small bits of data with low energy
iBeacon: Location-based service using BLE

1) Detect Beacons
2) Estimate distance
3) Push notifications and indoor localization

Check our new released product.
Drawbacks:

1) Requires hardware
2) Interval restricted by BLE Protocol
3) One hardware for each Beacon
4) Small Attack Range

Low Attack Efficiency and High Overhead
Wi-attack: Impersonation Attack from WiFi

High Efficiency with Low Overhead:
1) Utilities wide deployed WiFi APs
2) No Restrictions When Broadcasting
3) Large Effective Range
4) High Distance Error
Wi-attack

1) Enable Wi-Fi to BLE Communication
2) Attack Strategies in Different Scenarios
3) Enhance Attack Efficiency
1) Enable Wi-Fi to BLE Communication

2) Attack Strategies in Different Scenarios

3) Enhance Attack Efficiency
Large quantity of deployed tags

Wi-Fi Emulated iBeacon: Wibeacon

GFSK modulation

\[ s(t) = A \cos(2\pi(f + \Delta f)t) = A \cos(2\pi ft + \varphi(t)) \]
Spilt Encoding

Provides a packet reception ratio of 34.4%
1) Enable Wi-Fi to BLE Communication

2) Attack Strategies in Different Scenarios

3) Enhance Attack Efficiency
Attacks on Different Scenarios

- **Point deployment**
  - High Attack Success Rate for Every Scenario

- **Multilateral deployment**

**Attack Parameters**
- ID
- Reference Tx Power
- Transmitting Tx Power

![Diagram of WiFi and iBeacon deployment]

**Location of WiFi**
**Location of iBeacon**
Wi-attack

1) Enable Wi-Fi to BLE Communication

2) Attack Strategies in Different Scenarios

3) Enhance Attack Efficiency
Impact of Cyclic Prefix

Analysis of Low Packet Reception Rate

Correct decoding probability

\[ P = 1 - P(A)P(W|A) - P(B)P(W|B) \]
Impact of Cyclic Prefix

Symbol 1001

\[ \text{bit 1 } = \text{ bit 4} \]

Symbol 1010

\[ \text{bit 1 } \neq \text{ bit 4} \]

Need to drag the sampling point from B to A
Enhanced Emulation

Redundant emulated packets with 0.2us delay
Evaluation
Implementation

➢ WiFi Attacker AP: USRP N210 SDR, 100ms advertisement interval
➢ Standard iBeacon: HackRF SDR, 100ms advertisement interval
➢ User Device: iPhone XS and commodity BLE chip CC2650
Evaluation

Packet Reception Rate and Stability Comparison

Wi-attack provides a PRR of 66.7%
Evaluation

Point Deployment

➢ With a high reference power setting, the estimated results are greatly affected.
Using only 1 WiFi AP can give more than 10 meters distance error.

By setting the Tx power reference correctly, the user could be misled to most places in the area.
Adding more APs to attack could significantly increase the error.

Multiple impersonation greatly effects users in range.

Dynamic distance error is enlarged under WiFi attack.
Conclusion

• We propose Wi-attack, which reveals the feasibility of conducting impersonation attacks on iBeacon services using commercial off-the-shelf WiFi devices.

• Wi-attack provides an enhanced Wi-Fi to BLE direct communication which provides a high packet reception rate (up to 66.2%) and stability.

• We evaluate Wi-attack with 3 types of deployments. The results show that Wi-attack conducts a highly effective attack.
