Paper: Linking Bluetooth LE & Classic and Implications for Privacy-Preserving Bluetooth-Based Protocols

Summary: This paper investigates the vulnerability of Bluetooth Low Energy (BLE) advertisements and reveals that current Bluetooth chip design allows linking of BLE advertisements to Bluetooth Classic (BTC) frames and a globally unique identifier (BDADDR), leading to potential privacy breaches and de-anonymization. The authors demonstrate that the inference of the BDADDR from BLE advertisements is robust and can achieve over 90% reliability across apps, mobile devices, density of devices, and tens of meters away from the victims. It further discusses the implications of this vulnerability on privacy-preserving protocols and proposes several mitigations for the Android OS and Bluetooth stack to limit the attack's potential.

Strengths:

1. The attack performed to demonstrate the vulnerability of the BTC-BLE linkage is implemented over an extended period of time, about an hour, which shows that the attack is achievable and repeatable.
2. The use of a mobile app like Immuni as a BLE advertiser is representative of many contact tracing apps, making the results applicable to a wide range of apps on both Android and iOS platforms.
3. The paper has practical implications for app developers and device manufacturers, and the authors provide a library to enable developers to easily switch to a more secure BTC\_OFF\_BLE\_ON state.

Weakness:

1. Irregular transmissions and unexpected channel offset can affect the performance of the attack, making it less effective.
2. The attack also assumes that the separation between channels N, N+1, and N+2 remains constant, but this is not always the case. The presence of connectable or scannable flags in the advertisement can cause delays in advertising packets on subsequent channels, which can affect the accuracy of the attack
3. The experiments were performed in a controlled lab environment, which try to reflect real-world conditions. In real-world scenarios, there may be various factors, such as network congestion, interference, and other environmental variables that could affect the performance of the attack.