Paper: Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices

Summary:

This paper demonstrates various key challenges involved in finding a stable physical layer identifier to uniquely identify mobile devices using BLE protocol. In spite of BLE proximity application cryptographically anonymizing and periodically rotating the identity of a mobile device in their beacons, an attacker can bypass them by fingerprinting device at a lower layer. It shows how each of those factors limit accurate fingerprinting using a large scale field study consisting of 100s of uncontrolled BLE devices. The four factors identified through lab-bench experiments are: 1. BLE devices having varying chipsets with different Hardware implementation. 2. Some devices have lower SNR ABLe transmissions due to BLE transmit power being application dependent. 3. Major changes to physical layer impairments due to effect of temperature range on mobile devices in field and 4. accuracy difference between the low-cost receivers and the tools used in prior studies is not significant for RF fingerprinting. This reveals that BLE location tracking attacks can be a viable source yet unreliable at times to track mobile devices.

Strengths:

1. The devices taken for observation include not just mobile devices but also other products using BLE, which show coverage and effects of the study proposed across the device spectrum.
2. The method used for fingerprinting and identifying a target device makes use of the fact that a stable MAC address for a limited time duration yields the ability to receive multiple packets belonging to the same BLE device. This helps in identifying with more precision and reduces inter-packet noise. This is achieved using Mahalanobis distance which reduces the effect of small deviations in packet imperfections to give accurate fingerprints.
3. The data analysis around experiments conducted to determine false positives and negatives revealed how imperfections contribute to identification: CFO (carrier frequency offset) contributes the most to identification, followed by I/Q (in-phase/quadrature-phase) imperfections, and I/Q imperfections can help resolve the confusion between devices with similar CFO. Temperature can cause variation in CFO, while it does not have any notable impact on I/Q imperfections, which can help identify the target when it experiences temperature changes.

Weakness:

1. The approach taken to accurately measure BLE’s CFO and I/Q imperfections makes use of NAG. The optimization problem is not convex, which means that there is a possibility of converging to a local optimum rather than the global optima. Even though a threshold is used to determine whether the optimization has converged to an acceptable solution else the initialization values are adjusted to repeat the gradient descent process. This increase in computational complexity may require additional iterations to converge to the accurate estimations of CFO and I/Q imperfections. There’s a major tradeoff to choose between fine-grained or coarse-grained CFO estimation.
2. The countermeasures mentioned for prevention against the attack aren’t spoken about much. Specifically, improvements like chip design are something that would take substantial time to actually get released, and it’s not necessary that everyone would update their devices. Having a varying workload to keep a time-varying CFO, as suggested can lead to elevated device temperatures and a decrease in overall battery shelf-life.
3. The study conducted only evaluates the likelihood of false positives and false negatives for devices that were observed during one contiguous period of time in each location, which may not represent real-world scenarios where devices are in constant motion.