Bluetooth Operation Classification to Detect the Anomaly Behavior by Monitoring the Power Amplifier Signal

Abdelrahman Elkanishy

Motivation

Bluetooth is considered the most common choice for wireless communication in compact devices such as smartwatches, headsets, fitness trackers, and smartphones. In addition, through its extensive usage in Internet of Things (IoT) devices, Bluetooth has developed over the past 20 years to provide low energy consumption and high transfer rates which fit perfectly for area- and power-limited devices [1]. Due to the complexity of the integrated smart devices that use the Bluetooth communication protocol, most manufacturers are outsourcing the chips to third-party suppliers. The integration between many outsourced chips has resulted in the need to add a hardware security layer to ensure appropriate operation. For example, in Apple's smartphones, there is a dedicated a co-processor, Secure Enclave, to handle all cryptographic operations and maintain the integrity of data protection [2].

Manufacturers normally buy their Bluetooth chips from third-party suppliers, which are then integrated into a complex hardware-software stack with a variety of potential vulnerabilities. Direct measurement of the output and input power signals can help security functions prevent unauthorized data transmission. Bluetooth, as any communication protocol, has vulnerabilities. On the other hand, researchers disclose those attacks in order to provide security updates to defend users' devices. For instance, in 2017, Armis identified a new Bluetooth attack vector called BlueBorne that can take control of the target device. BlueBorne attacks regular computers, smartphones, and IoT devices [3]. This security breach occurs without pairing to the targeted device nor even while the Bluetooth is in discovery mode. As the Bluetooth chip is responsible for establishing the connection and controlling the flow of data, BlueBorne and other security breaches could attack the Bluetooth communication chip without consent of the controller chip. Therefore, monitoring a Bluetooth chip at the hardware level is necessary to verify its correct operation.

This project is part of bigger project which proposes a compact supervisory circuit to classify the operation of a Bluetooth chip at low frequencies by monitoring the radio frequency (RF) output and the power input lines of the Bluetooth chip. The idea is that classification algorithm can be inexpensively fabricated on a low frequency integrated circuit in legacy technology and/or with minimal area. When the supervisory circuit detects abnormal behavior, it can be configured to shut down the Bluetooth chip. Using features extracted from the power lines, we are able to train several machine learning (ML) algorithms to classify different Bluetooth operation modes and parameters such as operation profile, distance between the paired devices, and number of connected devices. Previously, we already investigated the RF output signals and trained ML models that can separate Bluetooth advertising and transmit/receive modes with ~ 100% accuracy and classify the operation profile of the Bluetooth chip with ~ 100% accuracy.

Problem

One way to monitor the chip is to consider it as a black box which consumes and transmits power. Thus, abnormal behavior can be detected by learning the normal input/output (I/O) power signatures or by parameterizing aspects of the Bluetooth connection (e.g., profile type, distance between paired

devices, and number of connected devices) and comparing to the controller chip instructions. For this project, I am aiming to inspect the power input of the power amplifier which drives the chip's antenna. Also, I will investigate can the Power Amplifier signal replace the RF signal to get the same classification accuracy. In this project, I will investigate another power signal domain of the Bluetooth chip which is the IVDD (Current Voltage Drain-Drain) of the power amplifier that drives the antenna. This power domain will be better for the electronic circuit implementation as it is not a RF signal. The measurement of RF signals requires to double the RF power in order to compensate the effect of power splitting. On the other hand, the IVDD measurement overhead only 1% of the power amplifier signal.

References

[1] K. Chang, "Bluetooth: a viable solution for iot? [industry perspectives]," IEEE Wireless Communications, vol. 21, no. 6, pp. 6–7, December 2014.

[2] iOS Security, iOS 11, January 2018. [Online]. Available: https://www.apple.com/business/docs/iOS Security Guide.pdf

[3] The Attack Vector BlueBorne Exposes Almost Every Connected Device. [Online]. Available: https://www.armis.com/blueborne/