Contents

1 TODO (2018 USENIX)Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors

1.1 DONE Summary

In this paper, the author utilize the resonance effect of MEMS inertial sensors to devise two different non-invasive spoofing attack toward embedded sensors. To conduct these attacks, the authors analyze the sampling process and find the way to control the digital signal output via changing the acoustic signal's amplitude, frequency and phase. To assess the performance of these attacks, the authors evaluate their attacks on 25 different devices and find 23 of them affected by the acoustic signal.

1.2 DONE Challenge

Previous works have utilized the ultrasound signal to attack the MEMS sensors in UAVs, however, they have a couple of deficiencies which are the main challenge of this paper.

1. The output of the inertial sensors are digital signals sampled from the analog signal generated by resonance and in real scenarios the sample rate of the ADC converters have some drift. The authors find that even little drift can affect the output of sensors significantly. So to control the output, the drift in sampling rate must be considered.

1.3 TODO Main Idea

1.4 TODO Strength

1.5 TODO Weakness

2 (2019 Wireless Communication)Localization and navigation in autonomous driving: Threats and countermeasures

2.1 Solved Problem

The paper contains two major parts.

- In the first part the authors make a comprehensive survey toward security vulnerabilities in today's state-of-art navigation and localization technologies.
- In the second part, the authors devise a novel route spoofing attack by injecting malicious code to modify the parameter of the route planning function in navigation apps.

2.2 Main Idea

The authors first construct a taxonomy about differentattacks on localization and navigation system. The maincomponents in these two systems are GPS and HD map. So,the authors classify different attacks base on their targetcomponent. For each sort of attack, the authors also discuss the countermeasures toward it.