R1 "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors"

Target system

Micro-Electro-Mechanical Systems(MEMS) gyroscopes

Target Service

Drones with resonant frequency identified.

Vulnerability

MEMS gyroscopes have resonant frequencies in both the audible and ultrasonic frequency ranges.

So, we can injected sound noise by an attacker.

There is no defense to prevent these resonant frequency attacks.

Exploitation

First, identify the resonant frequencies of MEMS gyroscopes used for drones.

As a result, there were resonance frequencies affecting drones in the X, Y, and Z-axes and only Z-axis.

They selected two target, one is affacting X, Y, and Z-axes and the other is only affected in Z-axis.

Then, they attached the Bluetooth speaker to the drones and turn on the noise.

They analyzed the effect of noise on the drones according to noise volume and distance.

Evaluation

This resonant frequency attack can physically damage the drones.

Not detected resonance frequency

- Frequency intervals were not sufficiently narrow.

Affected axes

- Target drone which affected axes are X, Y, and Z is successfully disrupted control.
  However, resonated only along the Z-axis drone is not disrupted control.

Attack distance

- The possible attack distance is approximately 16.78cm using maximum volume(113dB).
  This attack distance range might not be sufficient for an attacker.

Defense

1. Physical isolation
   - Surrounding the gyroscope with foam would also be a simple and inexpensive countermeasure.
   - However, this solution can raise the temperature of the board.
2. Differential comparator

- Using an additional gyroscope with a special structure that responds only to the resonant frequency, the application systems can cancel out the resonant output from the main gyroscope.

- Need an additional cost.

3. Resonance tunning

- By using an additional feedback capacitor connected to the sensing electrode, the resonant frequency and the magnitude of the resonance effect can be tuned.
- Resonant frequency still exists, so, attack is possible.

Future work

1. In experiment results, analog interface does not affect on this resonant frequency attack.

   So, I suggest that analyze the difference of the analog and digital interfaces.

2. Also, in software view, one countermeasure may be available.

   Manufacturer have to adjust the software, when the attack effect comes, it will return to the starting location. However, this solution has weakness. Since the gyroscope does not work, it can be difficult to move the drone to the correct location. Therefore, it is also required of accurate software modification.