# Vulnerabilities in Geofencing Strategies Used to Prevent the Flight of Unauthorized Aerial Drones in Restricted Airspace

Jack w. Barker - Supervised by: Konstantinos Markantonakis and Raja Naeem Akram

Information Security Group, Smart Card and IoT Security Center, NCSC funded

The Smart Card and Internet of Things Security Centre

## Objectives

The objectives of this project are as follows:

- To explore current methods in place to prevent unauthorized aerial vehicles from flying over restricted airspace.
- To exploit these vulnerabilities and determine the risk factors of each.
- Finding solutions to fix these vulnerabilities and to test them on a commercial drone.

## Introduction

Drones are becoming ever present in terrorist operations. This is evident in the numerous reports from Iraq where terrorist organization ISIS are using off the shelf DJI drones (RPAs - Remotely Piloted Aircraft) for use in Mosul against the Iraqi army. According to the University of Birmingham Policy Commission Report, these problems could be matched in the UK within 20 years as of 2014. A GCHQ director following this report has also reported that "Shopping centres, sporting events and public rallies face being exposed to chemical or biological attacks

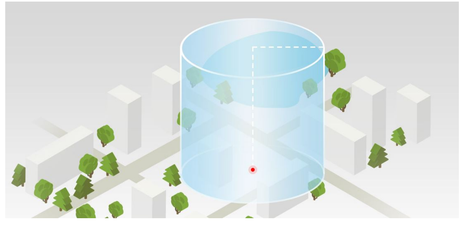

Figure 1: An example of a geofence used in an urban environment

## Equipment

The following Equipment was required to complete the research:

- Erle quadcopter drone.
- UBlox NEO-6m GPS module.
- Turnigy TGY-i6

When building the drone, I had to make sure that the GPS module was compatible with the micro-flight controller module.

## Challenges

One of the fundamental challenges was making the communication channel between the GPS module and the FC trusted so that a 3rd party cannot send false readings on the wire to the FC. This lead to me having tho create a signature scheme.

## Geohashing Method

Geohashing is a method of converting GPS coordinates into a hashcode in order to speed up the validation membership test in a list.

## Mathematical Section

Certificate authentication of GPS coordinate data. Firstly let Delta be the challenge list for the flight controller

$$\forall \delta \in \Delta, EKpubFC(\delta i) \rightarrow \varphi i \quad (1)$$

$$EKprivGPS(E\varphi(\delta i)(\mu i)) \rightarrow E\varphi(\delta i)(\mu i)) \quad (2)$$

encrypting delta of coordinate i encrypted with FC's public key with the private key of the GPS and the coordinate mu should give the challenge delta with the coordinate mu, hence the gps coordinate is validated

## Methods

One of the major vulnerabilities came from using a micro controller between the GPS module and the flight controller (FC) in order to trick the FC into thinking that it was in another location.
This lead me to create a signature scheme between the GPS module and the Flight Controller. This meant that each coordinate produced by the GPS module per second is validated by the flight controller to verify that it has come from the GPS module. See mathematical section as to how the GPS certificate works.

Figure 2: Quadcopter flying with GPS module

## Conclusion

To conclude, my research will prevent any unauthorized manipulation of GPS readings or hardware modifications on commercial drones. This in turn will lead to more safety over restricted airspace including airports, prisons and military bases as well as residences and private property.

## Additional Information

Take the latitudinal GPS coordinate 120.44734534. Estimating the circumference of the earth at 40,000km, and degrees to be 360, using the coordinate, the accuracy of the geofence will be a 110km box. increasing the point to 120.4, will result in a 11km box and so on. Increasing the accuracy of the GPS coordinates decreases the size of the geofence.

## References

[1] Donald E Knuth.
The complexity of songs.
*Communications of the ACM*, 27(4):344–346, 1984.

[2] Bhautik Joshi, Kristen Stewart, and David Shapiro.
Bringing impressionism to life with neural style transfer in come swim.
*arXiv preprint arXiv:1701.04928*, 2017.

## Contact Information

- Web: https://scc.rhul.ac.uk/
- Email: jack.barker.2015@live.rhul.ac.uk
- Phone: +44 (0)7549 606738