# UAV Attacked Through its Mission Plan

**Alexandria Garland**
**Mississippi Valley State University**
**9726 S 8th Ave**
**Inglewood, CA 90305**
**951-285-7035**
**Garland.allie@outlook.com**

## ABSTRACT
Unmanned aerial vehicles are used for missions that are too dull, dirty, or dangerous for human life. They have evolved to become an essential tool in the defense industry. Therefore, their security is essential. UAVs have vulnerabilities that have to be considered when deploying them. Cyber attacks are prevalent in a range of areas and now have been seen in the capture of UAVs. The 3DR X8+ is a popular UAV that handle a substantial payload and are great for capturing imagery. However, this UAV in particular has its own vulnerability that is exploited using a python script.

## CCS Concepts
**• Security and Privacy**

## Keywords
Gimbal; waypoint; UAV; drone; copter

## 1. INTRODUCTION
Unmanned aerial vehicles (UAV) are becoming popular amongst the defense industry as well as general population. For defense purposes, they are often used for missions that are too dull, dirty or dangerous for human life. Formerly, UAVs are predominantly used as Intelligence, Surveillance and Reconnaissance (ISR) platforms carrying payloads such as cameras, synthetic aperture radar, and signal intelligence systems. Surveillance over enemy lines and contaminated areas are just two examples of the UAVs purpose. Because they are used for important missions, security is essential. There are vulnerabilities on UAVs that have to be put into consideration before deploying them. The 3DR X8+, in particular, is a popular drone but it has a security issue with its autopilot.

## 2. UAV Attacks and Vulnerabilities

### *2.1 Waypoint Attack*

The waypoint attack modifies the waypoints in the autopilot's flight plan by causing it to fly a different trajectory from the one intended by the operator. This is the attack implemented by the python script which will be explained in more detail.

### *2.2 GPS Walk-off Attack*

When the UAV enters a pre-defined geographic region, the GPS location data is sent from the autopilot to the camera gimbal. The camera gimbal imagery is corrupted with slowly increasing bias. "The corrupted GPS data is included in the video stream as metadata that provides the coordinates of the area being viewed by the camera. As a result, the video imagery has erroneous position data associated with it and loses all value for ISR and targeting purposes (Heiges, Bever, & Carnahan)."



### 2.3 *Gimbal Command Attacks*

"The Gimbal Command Attack uses the gimbal command set to make the gimbal to appear to malfunction. When the aircraft entered pre-defined geographic region, spurious gimbal commands are issued to the gimbal causing it to retract or slew the sensor point of interest upwards. The gimbal retract command is issued whenever the aircraft is in the attack zone and the camera operator tried to engage the camera's tracking function (Heiges, Bever, & Carnahan)."

## 3. 3DR X8+

Figure 1: 3DR X8+

"The 3DR X 8+ is a ready-to-fly UAV that extends payload options to the professional realm." The payload capacity of 0.8kg, maximum take-off weight of 2.50kg, and flight time of 15 minutes(depends on payload weight, it varies). "The X8+ is optimized for GoPro aerial photo and video data. In addition, it has options for attaching an array of gimbals, professional cameras and sensors to the copter. This personal drone can generate highly accurate maps and 3D models, collect aerial data in automated and infinitely repeatable flight paths, gather data beyond the visible spectrum, generate point clouds for precision survey an can even be outfitted with magnets for real delivery potential. Its flight protection includes: redundant and durable design, an innovative motor system for reliability, and its fully-automated flight control for ease of use. It has an aluminum frame sturdy enough to take the elements but light enough to maximize aerial mobility. The frame folds into a compact and easily transportable from perfect for on-site use in a range of areas (X8+)." The ground control software used to control this UAV is Mission Planner.

## 4. Mission Planner Ground Control Station

Figure 2: Mission Planner Ground Control Station

"Mission Planner is a free, open-source, community supported ground control station for Plane, Copter and Rover platforms. The code for the application is written in C# and maintained by GitHub. It is compatible with Windows only. Mission Planner is a dynamic control supplement for autonomous vehicles. With this application, the user loads the firmware ArduCopter 3.2 into the autopilot, which controls the vehicle. It is used for setup, configure and tune the vehicle for optimal performance. The interface allows the user to plan, save and load autonomous missions into the autopilot with simple point-and-click way-point entry on Google or other maps, like Bing. After a mission, the mission logs created by the autopilot can be downloaded and analyzed. The application is interfaced with a PC flight simulator to create a full hardware-in-the-loop UAV simulator. With appropriate telemetry hardware, the operator has the capability to monitor vehicle status while in operation, record telemetry logs which contain much more information than the on-board autopilot logs, view and analyze the telemetry logs, and operate the vehicle in first person view (FPV)." To control the copter, there are different commands that are performed at, or on its way to different destinations, or waypoints. The commands include: "Navigation commands that are used to control the movement of the vehicle, including takeoff, moving to and around waypoints, changing altitude, and landing. DO commands are auxiliary functions and do not affect the vehicles position (for example, setting the camera position). Conditional commands are used to delay DO commands until some condition is met. During a mission at most one "Navigation" command and one "Do" or "Condition" command can be running at one time. (Heiges, Bever, & Carnahan)" Each of the commands is assigned an identification number, along with position/location information. For example, a waypoint command is identified as 16.

### *3.1 Autopilot*

The mission plan for the autopilot can be created on the Mission Planner Ground Station or a previously created mission plan can be chosen from the user's computer. In figure 2, the interface shows how the operator would create a mission plan. When the mission plan is created and saved, security measures (i.e. encryption) aren't performed on the data within the file. This data is in plain text. The first three lines of the file are for identifying that is indeed a flight plan for autopilot. The remaining information contains the details for the entire mission. This information is the locations and commands at each waypoint. For a mission, the user has to select the desired mission plan. This mission plan is loaded to the controller then to the copter. When the user selects autopilot on the controller, its flight path is based on the content within that selected mission plan.

## 5. Exploiting the Autopilot File

Through a series of black hat exploits, the attacker can obtain the autopilot files before they are deployed onto the drone, manipulate the data and return the file to its original location. If the operator of the UAV doesn't verify its autopilot flight plan, the UAV will be where the attacker requested. A python script is used to make the alterations to the flight plan. The python script first searches the computer for all mission plan files, the attacker then selects a file they wish to modify, then are given four options: change an existing command to a different command, edit an existing command, insert a command into the mission plan, and delete a command from the mission plan. The attacker has the functionality to make as many changes to the mission plan as he/she chooses before returning the file to its original location. After making the changes to the current file, the attacker has the option to change another file before exiting.

There are several concerns with being able to make these changes to the flight plan without the operator's knowledge. The UAV could fly to the attacker's home and captured or destroyed. It could be carrying high-level information that could pose a risk to national security. The X8+ could simply experience battery exhaustion on its way to the foreign destination and fall right out of the sky.

## 6. Conclusion

UAVs are becoming a major part of protecting our great nation. They are able to go where human life wouldn't survive to be the eyes and deliver a wide spectrum of payloads. However, their security is important when the mission is high profile. The python script could cause detrimental damage to the country if the payload is top-secret. Other attacks like actually obtaining the information from the UAV and using that data maliciously could cause grave harm to the country. On a domestic level, stealing someone's drone is illegal and subject to fines. Simple attacks with the python script are so small compared to the potential of many others.


#### ACKNOWLEDGMENTS

I would like to acknowledge my manager, Anthony Choi, and the lead on this project, Michael Roberts.


## 7. REFERENCES


[1] Heiges, M., Bever, R., & Carnahan, K. (n.d.). *How to Safely Flight Test a UAV Subject to Cyber-Attacks*. Retrieved April 1, 2016, from NATO OTAN: http://www.sercuarc.org/wp-content/uploads/2014/05/How2SafelyFlightTestUAVSubject2CyberAttacks-CSOSymposiumPaper-Heiges.pdf

*[2] X8+*. (n.d.). Retrieved April 1, 2016, from 3DR: https://3dr.com/x8/