20 Οκτωβρίου 2015

”Χακάροντας” drones: ένας νέος κυβερνο-κίνδυνος

/ Πεμπτουσία

Image not found or type unknown

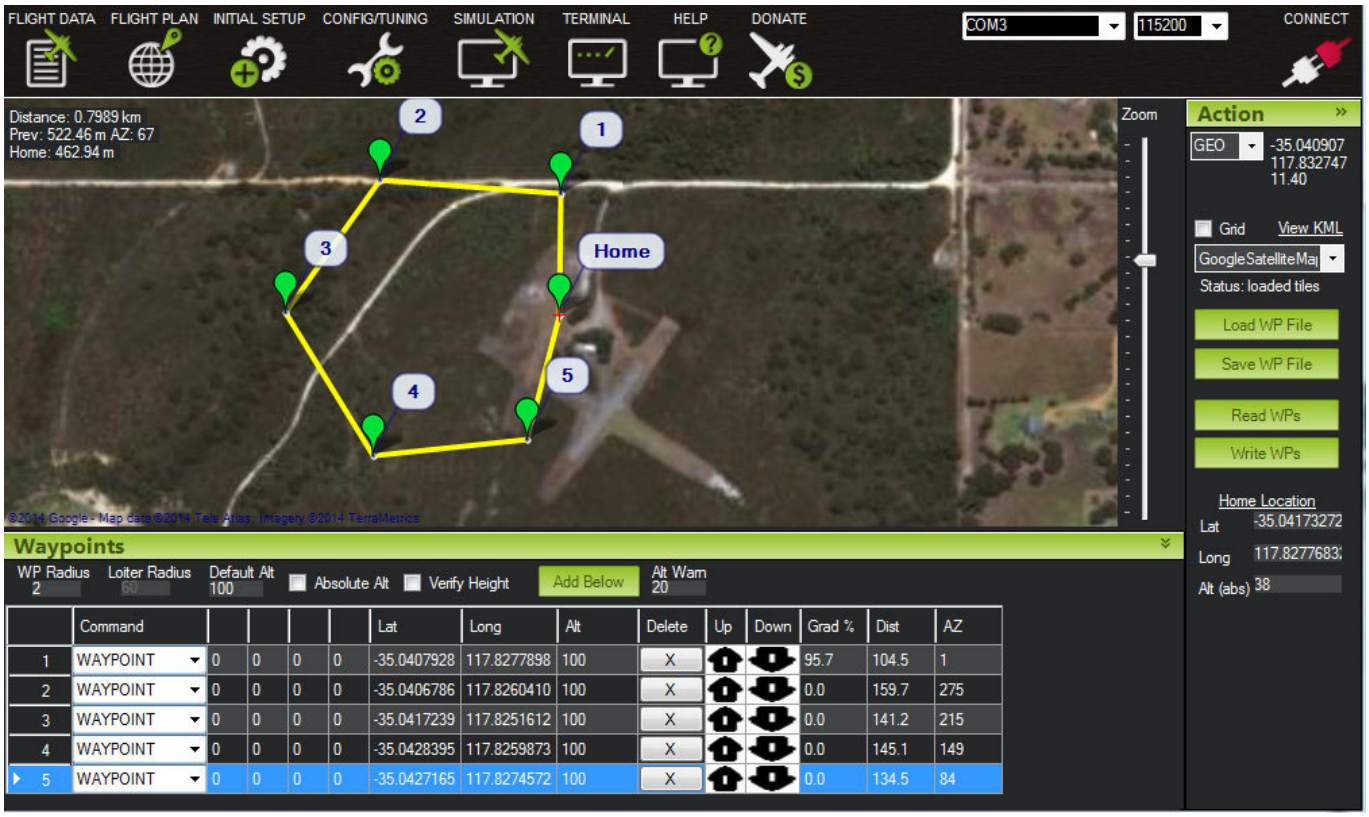
Η βιομηχανία των drones αναπτύσσεται με ραγδαίους ρυθμούς, κι έρευνες δείχνουν πως οι πωλήσεις τους θα ξεπεράσουν τα 89 δις δολάρια τα επόμενα χρόνια. Η ραγδαία εξέλιξή τους όμως εγείρει και αρκετές ανησυχίες όσον αφορά την ασφάλειά τους και φυσικά την απειλή που θα μπορούσαν να αποτελέσουν για την ιδιωτικότητά μας.

Στο συνέδριο Virus Bulletin 2015, ο ερευνητής ασφαλείας της HP Security Research, Oleg Petrovsky έκανε λεπτομερή αναφορά στις μεθόδους που θα μπορούσαν να χρησιμοποιηθούν για το hack των μη επανδρωμένων εναέριων οχημάτων [unmanned aerial vehicles (UAVs)], γνωστών ως drones, τα οποία εκτελούν προγραμματισμένες διαδρομές.

Ο Oleg Petrovsky έκανε επίδειξη του πως θα μπορούσε κάποιος να hackάρει ένα drone στοχεύοντας τον ελεγκτή πτήσης του και ανέλυσε τους ελεγκτές διάφορων multi-rotor drones και ανακάλυψε αρκετές αδυναμίες που θα μπορούσαν να αξιοποιηθούν σε cyber attacks.

Παρά το γεγονός ότι υπάρχουν πολλά διαφορετικά μοντέλα drones διαθέσιμα στην αγορά, τα οποία όμως αποτελούνται κατά κύριο λόγο από τα ίδια βασικά μέρη, συμπεριλαμβανομένων των παρακάτω: κινητήρες, μπαταρίες, αισθητήρες, μια μονάδα GPS, ένα remote control radio receiver, electronic speed controllers (ESC), και τον ελεγκτή πτήσης.

Ο Petrovsky κατά την έρευνά του επικεντρώθηκε στις επιθέσεις που έχουν ως στόχο τον ελεγκτή πτήσης, ο οποίος είναι ένα σύστημα που αποτελείται από διάφορους αισθητήρες και μια μονάδα επεξεργασίας. Η πλειοψηφία των drones χρησιμοποιεί τους ίδιους ελεγκτές πτήσης, όπως είναι τα ArduPilotMega (APM) και Pixhawk από την 3D Robotics, MultiWii, OpenPilot, και DJI Naza.



Ένας πιθανός εισβολέας μπορεί να επικεντρώσει τις προσπάθειές του στο hacking αυτών των controllers, ώστε να καταφέρει να στοχεύσει σε ένα ευρύ φάσμα μοντέλων. Ο Petrovsky χρησιμοποίησε για το test του ένα ArduPilotMega (APM) flight controller σε drone που έφτιαξε ο ίδιος και ένα Mission Planner, το οποίο είναι ένα ground station application.

Ο ερευνητής κατέγραψε με λεπτομέρειες μερικά σενάρια επίθεσης εναντίον drones με προγραμματισμένες διαδρομές χρησιμοποιώντας ground station software. Το ground station application είναι ένα καίριο συστατικό της πτήσης ενός μη επανδρωμένου αεροσκάφους, αφού επιτρέπει την επικοινωνία με την κεραία του οχήματος και επιτρέπει στο χρήστη να το ελέγχει ασύρματα.

Ο ερευνητής τόνισε την έλλειψη authentication στα πρωτόκολλα που χρησιμοποιούνται για τον εξ αποστάσεως έλεγχο των μη επανδρωμένων αεροσκαφών, η οποία θα μπορούσε να αξιοποιηθεί από εισβολείς για να αποκτήσουν τον έλεγχο των οχημάτων.

Παρόλο τον μεγάλο αριθμό ερευνών που έχουν πραγματοποιηθεί για το hacking των drones, ο Petrovsky εξηγεί πως δεν υπάρχουν σημαντικές βελτιώσεις όσον αφορά την ασφάλειά τους, και αυτό διότι δεν έχουν γίνει ακόμη real-world επιθέσεις σε εμπορικά μη επανδρωμένα εναέρια οχήματα.

Πηγή: secnews.gr