Cyber threats on un-manned aerial vehicles

K. Kathirvel 20394011, M.Tech NIS,
Pondicherry University, Puducherry, India

ABSTRACT

As we all know that the use of unmanned aerial vehicles nowadays is increased a lot because of the variety of its application. Due to increased usage of these unmanned aerial vehicles, it is mostly targeted by hackers. The use of poor security measures employed and lack of security mechanism it is like low-hanging fruit and one of the favorite target for attackers. This article gives an abstract idea of how the UAV's are hacked and its mitigations, how to prevent it by both legally and technically and some case studies. The problem here is attackers control the UAV which they don't own and use it for their malicious purpose. These UAV leads to damage of property and even sometimes leads to the loss of life. Nowadays these UAV are widely used by military, defense and law enforcement agencies. These leads us to number of questions like what happens if these UAV have been hacked? The cost we given for this is high so UAV needs to be secured and certain mechanism like anti-drone system need to be developed to defend us from enemies.

Keywords: UAV, SUAV, UAS, drones, cyber threats on unmanned aerial vehicle, security threats on drones etc.

I. INTRODUCTION

The sales of UAV's each year is keep on increasing because of users using it. In older days these UAV's are only used by military and government agencies, but nowadays it is used widely by all people around the world. For instance, Indian regulatory body Directorate general of civil aviation puts a ban on the use of civilian drones from 2014 to 2018. After December 1 2018, only civilians are allowed to fly drones with certain regulation. Every technology has their advantages and disadvantages, UAV's are also not excluded from it. It has variety of application including geographical photography, defense applications like carrying goods and supplies to allies, carrying weapons, monitoring enemies movement, aerial surveillance on suspect and used in disaster times etc., On other hand, it may be used by terrorist for monitoring army movements, boundaries, sometimes used to drop bombs to kill people, damage property by hitting on it, or just falling from certain height on someone may cause serious injuries to person, privacy intrusion, trespassing to un-authorized areas etc., Because of these capabilities, it is widely used and can be low hanging fruit to hackers. There are some incident that are recorded in history stating UAV's hacked and used for malicious intent by attackers. Sometimes our enemy nation can use this type of aerial vehicle to monitor and attack our nation. These force us to implement some counter measures like imposing no-fly areas, use of anti-drone systems, active and passive surveillance on our sky area. These are all well described with some case studies and examples.

II. UNMANNED AERIAL VEHICLE

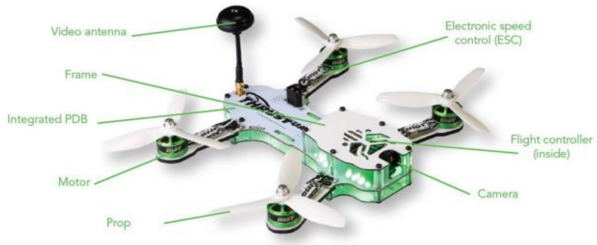
Unmanned aerial vehicle (UAV)/ Unmanned aerial system (UAS)/ autonomous or remotely piloted aerial vehicle, popularly known as drone is an airborne system which can be remotely operated or autonomously driven aerially. It does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload. It can also be driven autonomously without any operator by computer present in it with the help of GPS.

A. Components of UAV

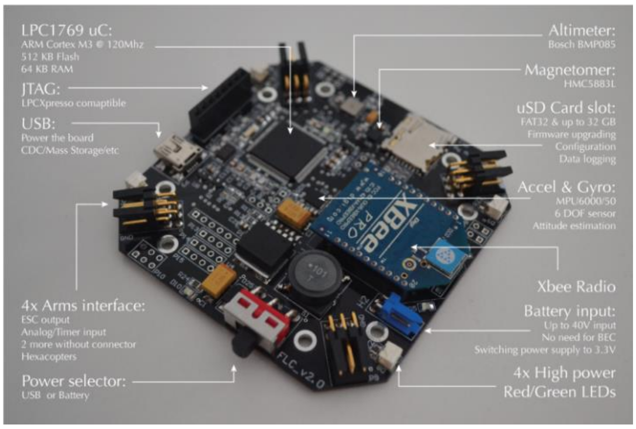
UAV is a flying device which comprise of both hardware and software. The hardware is responsible for flying whereas software is responsible for controlling the hardware. Hardware components includes motors, battery and some input devices. On the other hand, software consist of firmware or operating system which is tightly coupled with its hardware.

Hardware Components

The main hardware component of UAV is printed circuit board (PCB). PCB consists of several electronic components and variety of sensors which controls the flight operation, radio transceiver to transmit and receive radio signals through which it has been controlled on flight, motor and a propeller attached to it which helps it to fly by pushing the air towards down which effects in lifting it upwards as per newton third law of motion, GPS receiver for picking GPS signals, battery for supplying power to the components, rear and front-facing camera and microphone which helps for controlling and capturing of the aerial view, storage medium like SD card which helps to store the captured image/video.



The above picture is the overall components of the drone. But it contains some more components which are embedded into the printed circuit board (PCB) which is the control unit of drone.



The PCB contains various type of sensors based upon application of that UAV. Common sensors like accelerometer, gyroscope, barometer and magnetic sensor etc.

Software Components

Software's are the programs which helps to use the hardware component. Hardware is like piece of bare metal which we cannot do anything without appropriate software's. The firmware aka operating system which controls the UAV's. Most of the UAV's are equipped with flight OS which is made up of ROS (robot operating system) and Linux.

These make us to understand that UAV's are computer with flying capabilities.

III. THREATS BY UAV's

Threats are anything (e.g. object, substance, human, activity etc.,) which are capable of acting against an asset in a manner that can cause harm to humans or properties. Since UAV's are widely used due to its enormous number of application, unfortunately sometime it may be acting as a threat to the human lives also. The threats possessed by UAV's are payload attacks, signal hacking, privacy intrusion, insider threats, intrusion trespassing, civil disobedience, kinetic attacks, surveillance and espionage (spying).

In military, these UAV's are launched purposefully to kill soldiers and destroy their camp. These UAV's have been responsible for killing hundreds and thousands of soldiers in both battle area and their hiding place. Countries like china, Pakistan are spending millions of dollars in making UACV (unmanned aerial combat vehicle). China's Wing Loong is predator class UAV which is very larger in size and that can be controlled upon 4000km and can lift weight of

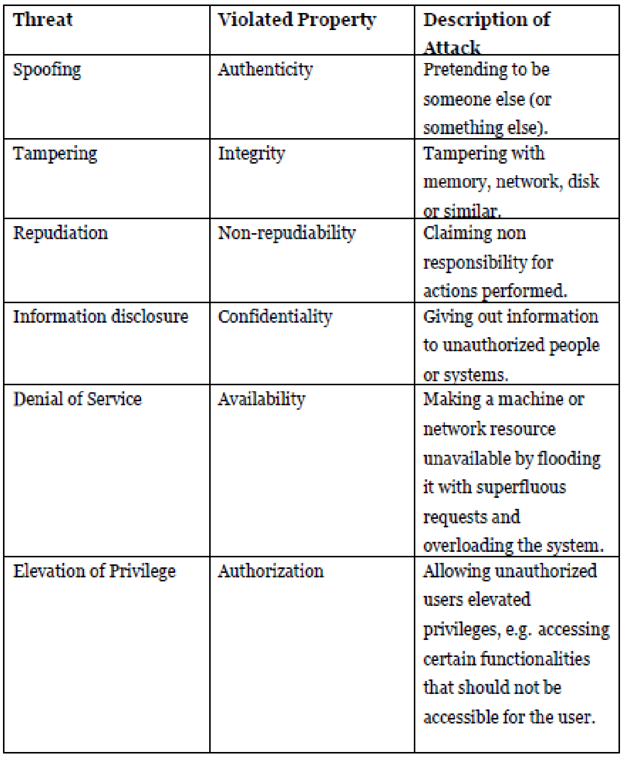
480kgs can cause desirable amount of damage to the enemies. These countries can do experiments on fixing small machine guns (SMG) in the SUAV (small unmanned aerial vehicle) which is small and fly over to the enemy and kill him with the SMG. The sci-fi short film named Slaughterbots describes very small UAV's in the size of a toy are filled with plastic explosives and flying autonomously on searching for defined targets using Image recognition algorithms and fly nearby them or land on them and blasts which definitely kills that person. Use of UAV for killing humans in not new, In August 1849 countries like Austria send nearly 200 hot air balloon with time bomb loaded on it to Venice, Italy to kill people flooded in streets of Venice to celebrate famous their carnival - Festa della Madonna della Salute. From these incidents we came to know that how UAV's are used to kill people in several battles.

IV. SECURITY THREATS TO UAV's

Cyberattacks are common to all electronic devices which has computing power. As already told that UAV's are flying computer or computing device with flying capabilities it is also susceptible to cyberattacks. Since unmanned aerial systems are growing industry and still not mature, it doesn't contains necessary security mechanism or policies which make them vulnerable to various kinds of cyberattacks. The vulnerabilities present in UAV's are exploited by attackers and it has been low hanging fruit to them. On recalling the history we came to know that there are number of cyberattacks happened against SUAV's. These SUAV's are mostly used by civilians for capturing aerial photos which are always targeted by attackers. Not only SUAV's, unmanned aerial system (UAS) which is used in military can also be attacked by the hackers. For example, the UAS named RQ-170 Sentinel used by central Intelligence agency (CIA), America is hacked by Iranian hackers and got down.

There are number of ways the drone can be hacked by controlled by attackers. Most common attacks are given as disconnecting UAV from controller by de-authentication attack, GPS spoofing, GPS jamming, man in the middle attack, geofence spoofing.

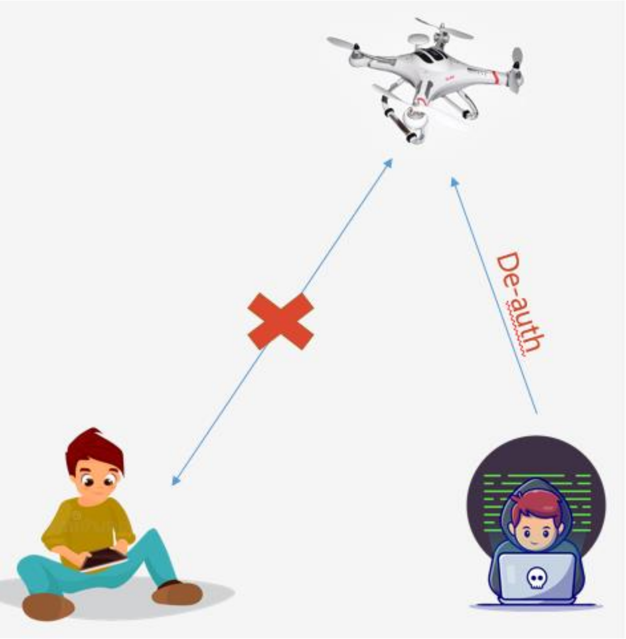
The below table shows that what security goals can be affected due to various types of attacks



Threat	Violated Property	Description of Attack
Spoofing	Authenticity	Pretending to be someone else (or something else).
Tampering	Integrity	Tampering with memory, network, disk or similar.
Repudiation	Non-repudiability	Claiming non responsibility for actions performed.
Information disclosure	Confidentiality	Giving out information to unauthorized people or systems.
Denial of Service	Availability	Making a machine or network resource unavailable by flooding it with superfluous requests and overloading the system.
Elevation of Privilege	Authorization	Allowing unauthorized users elevated privileges, e.g. accessing certain functionalities that should not be accessible for the user.

A. Disconnecting UAV from the controller

UAV's are remotely controlled flying object which can be controlled by using radio waves on precisely saying most of SUAV's uses 2.4Ghz wifi for communication between controller and them. Some of the UAV's also use 900Mhz for their communication.



These kinds of attacks can only be possible in UAV's which uses wifi for their communication.

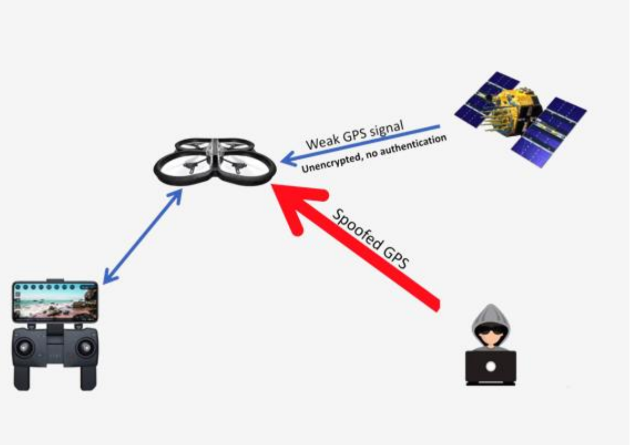
The attacker first monitors the wifi signal for any UAV. The attacker put his wifi adapter in promiscuous mode or monitor mode (The wifi adapter should support packet injection). Then attacker passively listens to the frequency and checks for the drone. It can be done by simply matching the OUI (organizational unique identifier) of the mac address of the drone with the mac address got from listening to the frequency. If it matches then the drone is found which can be deauthenticated. Then the attacker uses aireply-ng package to deauthenticates the UAV from the actual controller. Then the attacker itself can try to connect to the UAV and start controlling it. There is a script available online named dronehole which is available in github as opensource that automates all the steps mentiond above. Even a script kidie attacker can make use of this script to attack UAV and take control over it.

After the successful deauthentication attack, the drone may fall into the property or a person or land on the ground safely which can be stolen by attacker or modern drones has RTH (return to home) feature enabled so it returns to the previously save location autonomously by picking GPS signal using GPS receiver.

B. GPS spoofing

GPS (Global Positioning System) is a satellite-based navigation system. It provides time and location-based information to a GPS receiver, located anywhere on or near the earth surface. It works in all weather conditions, provided there is an unobstructed line of sight communication with 4 or more GPS satellites. GPS uses trilateration for giving location info to the user. GPS signals are weak, unauthenticated and unencrypted.

GPS spoofing happens when someone uses a radio transmitter to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal. Most navigation systems are designed to use the strongest GPS signal, and the fake signal overrides the weaker but legitimate satellite signal. Due to the weaker nature of actual GPS signal, it can be easily spoofed by sending strong GPS signal and navigation system are also use strong GPS signal only so that it takes our spoofed strong signal and use it for flight operations. GPS spoofing cause more damage to autonomous aerial vehicle rather than remotely piloted one. Because in remotely piloted aircraft system the control of the UAV is in the pilot’s hand.

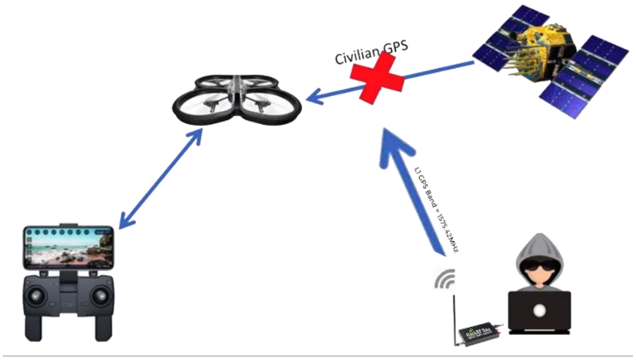


This is not a theoretical attack practically it has been done by Russian hackers, where they send false GPS data to the ships sailing in the red sea which affects the GPS receiver of the ships and showing as they are in the land.

C. GPS jamming

GPS jamming is the use of any frequency transmitting device to block or interfere with GPS signals. Due to the weak nature of GPS signals, Attackers can use any transmitting device to transmit a strong radio signal at the same frequency. So the GPS enabled UAV cannot able to receive the actual GPS information which affects the autonomous aerial vehicles. The autonomous aerial vehicle normally uses GPS signals to locate their location and destination location and follow their flight. If their GPS signal loses it losses its brain.

A few examples which through some more light on the GPS jamming are given as South Korea experienced GPS jamming attack which affects GPS navigation for passenger flights and ships and it blame north korea for the attack. UAV’s used by homeland security is tested and hijacked successfully by University of Texas students. Russia jams the GPS signals when US Fighter aircraft reaches approach Iran are the few examples that show this can be done already by attackers all around the world.



D. Man in the middle

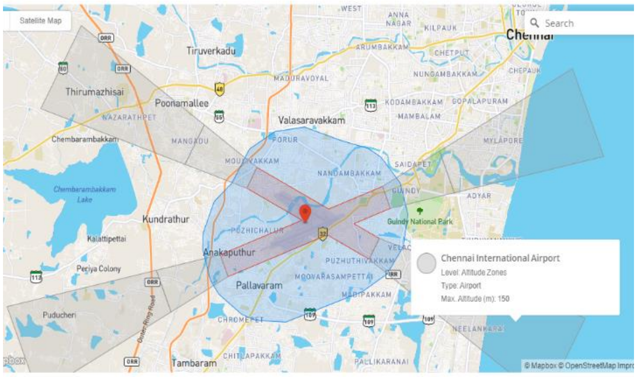
Man in the middle (MITM) is an attack that is a very older type of attack in local area network (LAN). This can be suitable for UAV's also where an attacker sits between the UAV and actual controller. Here attacker fools the drone that he is the legitimate controller. The attacker can modify, delete, insert the ongoing communication between controller and drone. This attack is possible because of the unencrypted communication between the controller and the UAV.

Here Attacker flies one UAV nearer to the target UAV which de-authenticating the target UAV from the controller and authenticates to the target UAV, pretending to be its owner and give commands to it. There is how swarm of drones can be controlled. The Skyjack is the project which demonstrates that a drone engineered to autonomously seek out, hack, and wirelessly take over other drones within wifi distance, creating an army of zombie drones under attacker control.

E. Attacking geofencing

Geo-fencing helps in making drones fly outside of the no-fly area. A no-fly area is a territory in which an aircraft or UAV are not permitted to fly. Geo fence enabled drone compares its position using GPS with the no-fly zone areas. It does not allow the drone to proceed if it gets close to the no-fly zone. The no-fly zone is set by the Government authorities

Here the attacker downloads the database of the no-fly zone from the drone. Modify the entries in the database and re-upload the database to the drone. Which bypass the no-fly zone restriction imposed by drone manufacturers. The below images show the no-fly zone.



F. Password theft

Password theft can be attacks that are done usually by brute force attacks and dictionary attack. In dictionary attack the use of dictionary file which contains the weak passwords like numbers in sequence, default passwords, common words and worst passwords on the internet. In Brute force attack attacker simply uses all combination of words and numbers to find the passwords. By doing so, if attacker gets the password then he/she tries to connect with the password to the wireless access point.

G. Denial of service

In a Denial of Service (DoS) the attacker takes can make the UAV's resources busy by giving continuous requests to it. For example the attacker tries to give connection request again and again or start to bombared the UAV using tools like hping3 he/she can cause the UAV's to halt thereby making the UAV fell down to ground. Sometime giving large password to connect to UAV may fill the buffer and can cause buffer overflow in the UAV.

H. Reverse Engineering

Reverse engineering is the method in which the attacker tries to reverse the binary to get its source code. In UAV if attacker reverse the binary and gets the source code and modifies it to something malicious and compile it to make binary then re-upload it to UAV using firmware update options. Then attacker can able to get control on UAV because of the modified malicious code put by attacker. Sometimes hackers use social engineering skills to make the user of UAV to download the malicious binary and when user updates using that malicious binary then attacker got control over it.

V. COMMON ATTACK VECTORS

The cyberattacks are not only limited to the above metioned but some other common attack vectors are still considered as threats to the UAV's. These include no authentication is used to connect to

drone, allows multiple users to connect simultaneously, the connection between drone and controller are not encrypted and multiple running services with vulnerability.

VI. COUNTERMEASURES TO UAV

Since the usage of UAV's widely, many Government all over the world tightening their laws to counter-fit the usage of UAVs for malicious purposes. Anti / counter drone systems are developed to address threats posed by drones. The first step in an anti-drone system is detection after that only necessary actions are taken to take down the UAV.

Missile
Predator Bird
Collision
Projectiles
Jamming
Geofencing
Catching
No-fly zones

The use of missiles, predator birds, projectiles with nets, jamming signals, geo-fencing, and launching another UAV in a way that it collides with the enemy UAV and even sometimes launching cyber attacks on the enemy UAV are some of the counter measures that can be used to stop the enemy UAV's.

Drone-killer fires microwave beams to disable UAVS

Radar Surveillance, Aquatics Surveillance, Video Surveillance, RF surveillance are used to actively detect the UAV's in critical zones like boundaries, war zones etc and they can be taken down using any of the above-mentioned ways.

VII. CONCLUSION

Unmanned aerial systems have a wide variety of applications, The more new application still needs to be explored and used as a boon for mankind. Each and every technology has its own merits and demerits. The use of these UAV's in a good way can lead to various improvements in human life.

VIII. REFERENCES

[1] A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles
2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR) Shanghai, China, October 11-13, 2017

[2] Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System
Ahmad Y. Javaid EECS Department
University of Toledo, Ohio ahmad.javaid@rockets.utoledo.edu
Weiqing Sun ET Department University of Toledo, Ohi
oweiqing.sun@utoledo.edu

[3] Unmanned aerial Vehicles: Vulnerability to cyber attacks
Springer Nature Switzerland AG 2020
K. Jain et al. (eds), Proceedings of UASG 2019