Cybersecurity Concerns in Surveillance Drones

Sana Sultan, Madawi M. Aldaweesh, Lina AlTayeb, Anees Ara
Computer Science Department
College of Computers and Information Sciences
Prince Sultan University
Saudi Arabia

***Abstract*— Nowadays, with the fast-growing need for surveillance, to ensure the safety and security of industries and people, aerial surveillance systems in this regard will be very effective. In this paper, we study and analyze the security aspects of drones in surveillance systems. This paper is divided into three sections; firstly we conducted a domain analysis which includes assets identification and prioritization, malicious actors and threats, and vulnerability identification. After the domain analysis, we conducted a design analysis that consisted of an architecture overview, the applied security, the security considerations, the external systems, an evaluation of the architecture, the security model, the machine and trust boundaries, and the assets mapping. After that, we conducted a security analysis where first we chose three subdomains which are GPS (Global Positioning System) module, the communication wireless network, and the flight Controller to be able to analyze the vulnerabilities of each subdomain, then we analyzed the reason why we chose these three subdomains. Lastly, we created a security checklist so that researchers in the future can come back to it at any time for reference.**

Keywords*— Surveillance drones; UAVs; Components; Security analysis; Architecture; Flight controller; GPS module;

I. INTRODUCTION

Drones, which belong to the UAV (Unmanned Aerial Vehicles) group, have certainly gained popularity in the past few years as they were once restricted for only military usage. Drones are currently used in the following fields: In agriculture, drones are used as a support tool for farmers to have a closer look on their farmland, Aerial Photography in the military field and the field of Journalism and photography, express shipping and delivery, Collecting information or providing necessities for disaster management, Drones with thermal sensors for searching for lost or wounded soldiers, Geographical mapping of inaccessible land and locations, building safety examinations, accuracy crop monitoring, unmanned shipment transport, law enforcement and monitoring at borders, tracking storms and predictions of hurricanes and tornadoes[2]. Increasing work efficiency and productivity, decreasing workload and cost of manufacturing, increasing accuracy, optimizing service and customer relationships, and solving security concerns on a large scale are some of the top uses of drones to offer global industries. Drones have become used more by civilians in different fields; therefore this creates a lot of new security risks that should be considered. In this report, we are going to focus on the use of drones in surveillance. The employment of drones for security surveillance was first restricted only to the military sector. Nowadays its use for security surveillance is starting to be wider where it became available in different fields like commercial and public fields. Using drones for security surveillance purposes solves all the issues that were faced when using traditional methods for security surveillance such as fixed surveillance cameras which required security responders to perform on-site investigations which wastes time and puts these responders in unsafe situations and helicopters which are extremely costly. The use of drones makes Data collection faster, more cost-effective, and more efficient.

Currently, in the following industries, drones are used for security surveillance purposes:

- Remote Area Inspection
- Traffic Surveillance and Management
- Maritime Surveillance
- Risk Assessment
- Inspections
- Perimeter Control
- Railway Surveillance
- Anti-poaching Operations
- Event Security
- Accuracy crop monitoring in the agriculture field (Drones are used as a support tool for farmers to have a closer look at their farmland and to monitor the crops.)
- Monitoring land and animal populations
- Ensuring the protection of groups of people (most likely to be important people like people with high positions in the country) and sensitive locations
- Military observation of unfamiliar areas/buildings in war zones

Although drones have many critical industrial applications, but there is no prominent research work addressing this problem. In this paper we try to investigate this area thoroughly in various aspects and fill in gaps by conducting a detailed security risk assessment and security analysis.

The major contributions of this paper are as follows:

- We conduct a thorough domain analysis and identify the security threats vulnerabilities and risk by mapping them with the asset inventory.
- We study the architecture and design of the drones in surveillance systems and figure out the critical assets and their locations with respect to security boundaries.
- We make security analysis of subdomains in these surveillance systems and propose recommendations for future purposes.

The remaining paper is organized as follows: section II includes, domain analysis, section III includes security analysis, section IV includes security analysis and finally section V concludes the paper.

II. DOMAIN ANALYSIS

Drones, on which our research is focusing, are considered as an application of CPS (Cyber-Physical Systems). Drones, belonging to the UAV category, have gained popularity in recent years as they have once been limited for military use only. They are currently used in the following areas: as a support device in agriculture for farmers to take a closer look at their farmland, aerial photography in the military sector, in the sector of art and journalism, express shipping and distribution, collecting information or disaster management needs, drones with thermal sensors to search for missing or injured soldiers, spatial mapping of inaccessible land and places, building health inspections, accuracy monitoring of crops, As drones are widely used in many sectors, the users, purposes, business objectives, and the process will differ as well. When it comes to the users, they use drones for different purposes. Each of the users seeks different goals to be achieved through drones, and for this reason, drones must perform their intended job while keeping their security as a high priority. Keeping the development team, including the security group, up to date on the possible drone threats and attacks is as important as the drone's production process. Indeed, there are a huge number of vendors or manufacturers of drones such as DJI, Yuneec, UVify, Hubsan, Parrot, etc., but this chapter does not focus on a specific one, rather discussing the threats and vulnerabilities to drones assets in general.

A. *Assets Identification and Prioritization*

A drone in very simple words is a flying robot that can be remotely controlled, and it consists of many sensitive and important components and data as shown in Fig. 1 and should be protected from malicious attacks, and unauthorized access and control. The main components that should be protected to ensure the security, availability, and efficiency of the drones as CPS especially for surveillance uses, are electronic speed controllers, flight controllers, receivers, transmitters, GPS (Global Positioning System) Module, and Camera. From these components, we can figure out more drones' assets which are the data and information that are recorded, collected, stored, and retrieved from these components.

All these assets that are mentioned above can be valuable targets for the attackers to exploit them either to gain sensitive info or harm the system. Also, attackers can deny the services by taking control of the flight controller and interrupting the signals that are sent and received by the drones' components. Since drones are a new technology, they have been around for two decades only; there is no old or not-needed component yet. But some suggested components could be added in the future to enhance the performance and security of the drones. For instance, Ethernet could be used in the future with drones to provide more secure network connections, and sophisticated sensors to enhance the accuracy of recorded data such as maps, videos, and pictures.

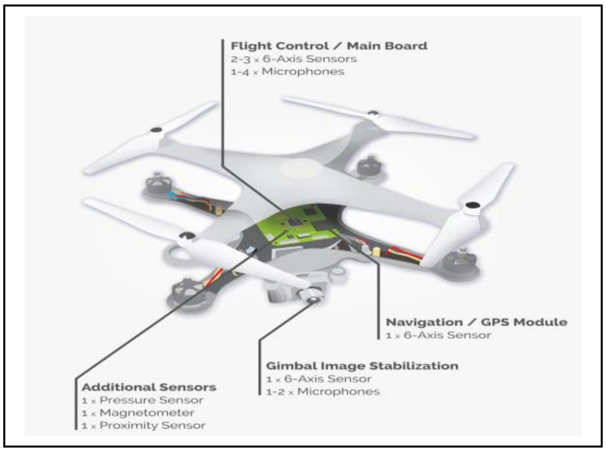

Fig. 1. *Example of UAV components [31]*

To prioritize these assets according to the severity of the consequences if it is compromised, the GPS module and radio signals come with high priority. GPS module in drones which is responsible for the provision of the drone longitude, latitude, and elevation points, enables the drone to travel longer distances, recording images of different land locations, it even allows to easily return "home" to the drone, any harm to this system can cause a huge loss. If the GPS has been compromised or exposed to any kind of attack such as spoofing or jamming, the drone will be lost from its original location then it could be in the hands of unauthorized people, and if the attacker could spoof the radio signals, he will take the control over the drone which ends with full access of the system including the other assets. As to why it is considered important.

In the second place, the flight controller, transmitter, and receiver are considered one of the most important assets. The flight controller is a motherboard that is responsible for all the instructions which the pilot sends to the drone, and the transmitter and receiver which transmit and receive radio signals from and to the drones play a significant role. They operate drones' main functionalities and perform the computations to give the right actions, so if they are compromised, they will come up with wrong decisions which cause serious and dangerous risks that could lead to human and financial losses.

The third priority is ESC (Electronic Speed Controllers) which is an electronic circuit that controls and regulates an electric motor's speed. Any attack that has a direct or indirect impact on ESC could be huge harm to the physical part. For example, if an attacker has gained access to this circuit, he can change the speed which causes defects in the process.

The least priority is the camera. Its importance lies in the feature that allows anyone who could gain access to it, to have a full picture of the current situation in the area it is worked in since it provides live recording for the real environment around the drone. Cameras should be protected from deactivation to ensure availability, and from data, theft to ensure confidentiality.

B. *Malicious Actors and Threat Identification*

In this segment, we will address the malicious attackers that Drones system can be In this segment, we will address the malicious attackers that Drones system can be exposed to and should protect it from itself, and categorize them according to the STRIDE (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of Service and Elevation of privileges) threat model, which is an acronym that stands for six different kinds of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. All these threats breach the desired property, in the same order as above, for most systems: Authenticity, Integrity, Confidentiality, Availability, and Authorization.

The most common attackers can be as follows:

- Password theft, which is conducted by an identity thief and can be carried out using various techniques, including dictionary attacks, brute force attacks, and statistical attacks.
- MITM (Man in the Middle), is a method in which the attacker monitors the communication between two parties and accesses (and can alter) confidential data without the knowledge of the attacked users.
- DOS (Denial of Service) assault against a UAV could be de-authentication requests that are sent at a rapid pace continuously, which can prevent any contact with the UAV.
- GPS Jamming and Spoofing attack produces signals in GPS jamming that conflict with the GPS signals, causing the GPS receiver in the UAV to malfunction. GPS spoofing is a similar but more complex attack; the attacker generates an erroneous signal instead of creating interfering signals that can cause the UAV to alter its location [1]. Some types of information are available to attackers. For example, MITM can gain the address information when sending broadcast packets inside the radio network, the addresses can be retrieved from the UAV, the UAV will then send an acknowledgment message containing that information, while in password theft the data required for this technique to work can be obtained from' leaks' in the targeted object's initialization vectors. Drones use GPS for navigation, and they are easy to hack since civilian GPS signals are not encrypted. There are many ways that malicious actors find vulnerabilities in drones' systems and exploit them. In a 2016 study, Rodday et al. conducted a MITM attack on a UAV. This attack exploited communication network vulnerabilities, in this case, the radio connection [1]. DOS attacks can be carried out by scanning mid-air UAV ports to identify vulnerable or open ports in the network so they could exploit the vulnerabilities in the system. Also, the password can be cracked by exploiting the weaknesses in the communication system to get access to the device and using the ROS (Robot Operating System) tools, for example, for controlling it. As GPS signals are not encrypted; they are easy to spoof [1]. To have a better understanding of the threats above, we can use the STRIDE threat model and relate the threats with CIA (Confidentiality, Integrity and Availability) components as follows:
- Cracking passwords to access a device is an Authentication breach and thus this attack may be considered as a Spoofing Identity.
- MITM and GPS Spoofing attacks can be classified as Spoofing Identity in STRIDE because they cause a breach of authentication to access user remote control and system UAV interaction.
- The DoS attack is already in the STRIDE model to crash the UAV and intended to harm the drone's system availability [1]. We conclude that spoofing and denial of service attacks are the most common types of cyberattacks against UAVs and that hijacking and crashing is the most common outcome of the attacks. Hijacking (taking complete control of the flight path) and crashing the UAV at will are the most common targets for hacking UAVs and because of this goal, most of the attacks fill in the two categories, spoofing and Dos attacks.

C. *Vulnerability Identification and Quantization*

In this segment, we list out the Drones' vulnerabilities as follows:

- In 2016, Rani et al. carried out a cyber-assault on a Parrot AR [1]. Drone as an example of how to take full control of a UAV, and revealed some vulnerabilities in commercial UAVs. There are several vulnerabilities found in drones (specifically in commercial UAVs) like weaknesses in the communication system which in the case of a Parrot AR. A drone is based on a Wi-Fi network that is built in the UAV, so attackers can easily gain full access and control over the drone by simply cracking the password using a password cracking tool called Aircrack ng, which works on de-authenticating legitimate users and giving control to attackers instead, to hack the Wi-Fi as legitimate users gain access and control over the drone by simply connecting to the Wi-Fi.
- A 2018 study by Dey et al. investigated what the current security situation is within today's UAV by hacking two types of drones; one was DJI's Phantom 4 Pro and the other was Parrot's Bebop 2 [1]. They concluded they're vulnerable to different types of attacks. Spoofing can be easily performed on Phantom 4 Pro drones as these kinds of drones use GPS for navigation and civilian GPS signals are unencrypted and so can be effortlessly spoofed. Open Wi-Fi is another vulnerability that is found in Bebop drones where open and unencrypted Wi-Fi is available and it also grants multiple users the ability to connect to the network which makes the validation process of the drone owner impossible. This vulnerability can be exploited using spoofing attacks.
- In a 2016 study, Rodday et al. conducted a man-in-the-middle attack on a UAV. Weaknesses in the communication system, this time especially in the radio link where knowing the selected connection parameters can hack the link and that can be easily achieved as nearly all of them are still set to their default values, and are thus easy to search for [1].
- Junia Valente, a Ph.D. software engineering candidate at the UT (University of Texas Dallas) found the bugs last fall through UT's Cyber-Physical Systems Protection Lab, a computer science program at the

school that offers IoT devices to students. Work by Valente, performed under the direction of Dr. Álvaro Cárdenas, concentrated mainly on the health of these devices. US-CERT (United States Computer Emergency Readiness Team) issued an alert last month about the quadcopter of DBPOWER U818A Wi-Fi [1].

The DBPOWER U818A quadcopter drone provides FTP (File Transfer Protocol) access through its local access point and requires the anonymous user to have full file permissions. The DBPower U818A WIFI quadcopter drone runs an FTP server that allows anonymous access without a password by default and provides the anonymous user with complete read/write permissions for file systems. Furthermore, the DBPOWER U818A WIFI quadcopter drone uses BusyBox 1.20.2, released in 2012, and may be vulnerable to certain documented bugs in the BusyBox. Similar models from other suppliers were later stated to appear vulnerable to the same vulnerability, but according to the researcher who documented the vulnerabilities, these similar models are produced by the same company but marketed under different names (This piece of information has not been confirmed by the CERT/CC.) After researching a lot in drones' vulnerabilities, we discovered that the most commonly occurring vulnerabilities are:

- Weaknesses in communication systems.
- GPS navigation system vulnerabilities (civilian GPS signals are unencrypted).

The maintenance of the CIA is key to the security of any system. Most Drones are embedded with GPS navigation systems where GPS signals can be doubtlessly spoofed as civilian GPS signals are unencrypted. PS navigation systems depend on sensors with external references. The usage of sensors with external references places a risk on the integrity of the system. If these sensors with external references are used to monitor critical sectors, this appoints a risk to the availability of the system. Most vulnerabilities will probably place both the integrity and the availability of the system at risk as the sensors with external references that the GPS navigation systems depend on will be most probably used to monitor critical sectors (for critical purposes): like military observation, railway surveillance, inspection, event security, protection of people with high positions in the country, etc., where drones are used for surveillance.

We discovered that most of the vulnerabilities exposed in drones are not specific to drones, as most of them are related to weaknesses in communication systems (Wi-Fi network problems, default passwords, etc.) and vulnerabilities in GPS navigation systems, and both of these systems are available in a lot of different domains and so have the same vulnerabilities in them. In our case, they are embedded in drones, in other cases, they may be embedded in other domains like smartphones for example, and as a result, will be hacked in the same way. For example, if the GPS application in an individual's phone is exploited then this will put the individual's life at risk and danger (he/she will feel unsafe) as very critical information about them has been exploited (the individual's current location).

The conclusion we came across is that the vulnerability frequency didn't change over the years as it was reported that the vulnerability to ARP (Address Resolution Protocol) Cache poisoning on the old drone's platform still exists on the new platform, on the other hand, a new sector of unreported vulnerabilities was discovered on other platforms. This shows how security measures are of no importance for commercial drone manufacturers as the vulnerability to ARP Cache poisoning has not been mitigated and still exists on the new drone's platform. Additionally, new unreported vulnerabilities in other platforms have arisen, and as a result, users are put at risk of being attacked at any time. Measuring the vulnerability impact is extremely important for risk assessment. We use the formula to measure the vulnerability impact using three steps:

1) Create Vulnerability Rating Table

This table designates a rating score for identified vulnerability, where the rating score ranges from VR1 to VR5 (very low to very high) based on specific standards.

VR– stands for vulnerability rating
VR1– stands for very high
VR5– stands for very low

TABLE I. VULNERABILITY RATING

Vulnerability Rating		
Score	**Criteria**	**Description**
VR.5	Very high	One or more major weaknesses have been identified that make the asset extremely susceptible to an attack. The organization has no capability of resisting the occurrence of the threat
VR.4	High	One or more major weaknesses have been identified that make the asset highly susceptible to an attack. The organization has the low capability of resisting the occurrence of the threat
VR.3	Medium	A weakness has been identified that makes the asset moderately susceptible to an attack. The organization has the reasonable capability of resisting the occurrence of a threat.
VR.2	Low	A minor weakness has been identified that slightly increases the susceptibility of the asset to an attack. The organization has a good capability of resisting the occurrence of a threat.
VR.1	Very low	No weaknesses exist. The organization has an excellent capability of resisting the occurrence of a threat.

2) A-VIAM (Asset Vulnerability Impact Assessment Model)

It is used to discover the impact of the vulnerability on the specified asset. This model is based on a formula that sums up the vulnerability rating scores of all the different vulnerability ratings and divides the sum over the total number of vulnerabilities.

$$V1(CA) = \sum_{VR=1}^{n} \frac{V_{VR1} + V_{VR2} ... + n_{vrn}}{total\ number\ of\ vulnerability} \quad (1)$$

Equation (1) shows the calculation for the A-VIAM model and is described as follows:

VI stands for Vulnerability impact
CA stands for critical asset
The results' scope is from 1-10
The result shows the vulnerability impact of the critical asset.
Where:
1.00–3.99 = low
4.00–6.99 = medium
7.00–10.0 = high

To compute the vulnerability impact of a whole system, the following formula should be used:

$$V1(S) = \sum_{VA(CA)=1}^{n} \frac{V1(CA1)+V1(CA2)\ldots+V1(CAn)}{total\ number\ of\ assets} \quad (2)$$

In (2), S stands for Overall Critical Infrastructure System. The result of the vulnerability impact of a whole system ranges from (10-100)% Example:4.8

3) *Identify Threats*

This step works on discovering the threats that the uncovered vulnerabilities may have caused [22].

With the completion of domain analysis, we found that drones have many security threats associated with their different assets, and based on their importance and the severity of their consequences if they are compromised, we prioritize them. Moreover, we highlight the different various vulnerabilities inherited in the drones' assets, and which attackers can exploit and attack the system. We found that most of the threats were limited to two types, either Dos or spoofing attacks. Plus, most of the drone vulnerabilities are related to weaknesses in the communication system and vulnerabilities regarding the GPS navigation system.

III. DESIGN ANALYSIS

In this section, the UAV architecture will be identified and analyzed thoroughly. The process starts by getting an overview of the various drone subsystems and discussing the security considerations for each subsystem. Also, this chapter will discuss the evolution of UAV architecture over time. In addition, a security model is picked and evaluated to show the external systems which have effects on the drone's subsystems and the machine and trust boundaries in between. As the last step, assets of the drone's system, which were mentioned in chapter one, were mapped to the architecture subsystems.

A. *Architecture Overview*

UAV is a term that describes an aircraft that can fly without a pilot; that is, an airframe and a computer system that incorporates sensors, GPS, servos, and CPUs (Central Processing Unit). Both of these components together must be piloting the plane without any human intervention.

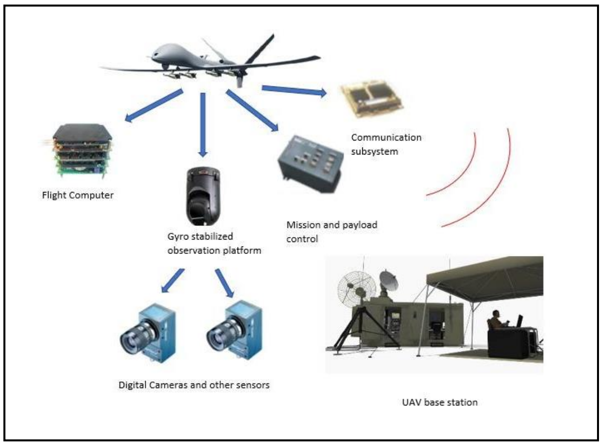
Flight Computer
Communication subsystem
Gyro stabilized observation platform
Mission and payload control
Digital Cameras and other sensors
UAV base station

Fig. 2. *Main components of a UAV system [19]*

UAV is effectively manned automatically by an embedded computer called FCS (Flight Control System). This is a device that reads information from a wide range of sensors like accelerometers, gyros, GPS, and pressure sensors, and drives the UAV trip along a predetermined flight path. We consider new hardware/software architecture specifically designed to act as a mini/micro-UAV mission and payload controller. A UAV is a complex device consisting of six main sub-modules, which function together to achieve a highly useful observation platform. In Fig. 2, we discuss what are the sub-modules included

- Airframe UAV, a plain, lightweight, aerodynamically effective, and secure platform, with limited avionics space, and no pilot room.
- The flight controller (core of the UAV), a computer device designed to collect aerodynamic information through a series of sensors (accelerometers, gyros, magnetometers, pressure sensors, GPS, etc.) to automatically guide an airplane's path along with its flight schedule across multiple control surfaces in the airframe.
- The payload, a series of sensors consisting of TV cameras, infrared sensors, thermal sensors, etc. to collect information that can be partly processed on board or transmitted for more analysis to a base station.
- The mission/payload controller, a computer system that has to monitor the operation of the sensors included in the payload inside the UAV.
- The base station, a ground computer system capable of tracking the progress of the mission and ultimately controlling the UAV and its payload.
- The communication infrastructure, a combination of communication structures including radio modems, sitcoms, microwave connections, etc. that should ensure the continuous link between the UAV and the base station [18].
- The communication manager or gateway monitors and restricts all communication links and traffic routes between the UAV and the base station through one or more connection channels [19].

B. *Applied Security*

As we don't discuss a specific drone brand in this paper, we can not specify the security applied to drone components. However, we can predict about the components that need encryption or authentication mechanisms to provide the minimum level of security for all drones. The base station needs authentication techniques as it can be accessed physically by malicious attackers or cyberattacks as well. In addition, the communication infrastructure, including wireless communication, needs to be protected by encryption mechanisms to prevent eavesdropping or signal spoofing attacks. The flight computer, as it is considered the heart of the drone, needs to be protected in the first place as it is responsible for all other drone operations.

Some systems are more susceptible to vulnerabilities, and thus being attacked. For example, attacks at the ground base station and the flight controller can be like the flight controller's operation depending solely on the information obtained through the data link in the communication infrastructure, from the ground base station and acquired from the surrounding environment by its sensors. Accordingly, attacks on both the flight controller and the base station that do not involve the data connection are only possible if the intruder can access and exploit the internal device communication or produce the sensed physical properties in the area around. Additionally, the payload and the communication infrastructure, containing the GPS receiver, can be a target for spoofing attacks as UAV navigation relies on the GPS signals the onboard GPS receiver receives and processes. GPS transmissions are unencrypted and unauthenticated signals which are freely available for civilian use. The transparent design of the GPS signals helps to spoof attacks.

C. *Security Considerations*

Drones as CPS are used for many critical purposes which makes security in drones a focus of attention, and it is built in both cyber and physical systems to prevent the occurrence of major risks such as security violations and human and financial losses. Such as but not limited to, in the base station which is essentially a computer device that connects with Wi-Fi compatible devices and is managed by humans, it is secured by using authentication authorization, and anti-virus is installed and a firewall. Also, to secure the physical part in the drones, a physical tamper resistance is used.

Drones, like all smart devices, are open to possible attacks. Security analysts have found that many commercial drones and certain industrial drones have significant bugs that could compromise them up to a mile away, and an attacker exploits these bugs and damages the whole system based on the risk level of the attack. Such flaws pose important concerns of protection and privacy for customers and companies because these attacks will decrease or destroy the functionality of the system. So any compromise of one component impacts the security of the device as a whole. For example, a DDoS (Distributed Denial-of-Service) attack that targets the cyber system in the drones ends up with many problems in the physical parts such as preventing authorized users from controlling the system. On the other hand, if the physical part has been compromised the cyber part is more likely to be affected. For example, theft of the device makes the attacker able to take control of the whole system including the cyber part.

D. *External Systems*

Drones are always interacting with different external systems to provide specific services and so these external systems sometimes tend to put the drone system at risk. Due to the fact that drones are widely used in critical systems like in military surveillance as they interact with military systems, this puts the drone system at a huge risk of it being attacked by enemies for political reasons. There is no doubt that drones have significant public health uses. They can be used to transport blood, tests, and biologics, such as vaccines to remote areas, and to minimize travel time. They can be used in disaster relief, and they can save lives. The interaction of drones with external systems like health care systems, in this case, might put drones at risk as drones used for medical purposes may be attacked by armed forces thinking it's a military drone (used for military purposes). Drones can be also used as flying base stations to provide communication services. For example, the interaction between drone base stations and terrestrial base stations to provide communication services can have several challenges and so imply risks on drones like providing robust and high-throughput backhaul as the drone base station needs to serve a big quantity of UEs and so the data rate and throughput of the backhaul connection will be high which can affect the drone's system performance.

E. *Evolution of the Architecture*

As drones are always evolving day by day, their architecture also needs to change so that it can evolve and offer more effective and secure services. Drones have become used in all different kinds of sectors nowadays due to their flexibility and advantages and so security challenges have increased with their wide usage in all the different fields. The fear of amateur drones being used for malicious purposes, confirming that drones are not flying in the "No-Fly Zone", the collision of drones all impose the idea of making changes in the current architecture of drones. To try to solve these security challenges, MDr deployment (Monitoring drone deployment) has to be achieved. To be able to capture amateur drones, MDr deployment has to be able to accurately perform the following functionalities: detection, localization, tracking, jamming, and hunting of amateur drones. The most critical facet of the deployment of MDr is the MDr architecture. Different MDr architectures are proposed according to the different levels of criticality and sensitivity of the systems. The point-to-point architecture was suggested for not highly sensitive systems and FANET (the Flying Ad-hoc Network) was suggested for use in highly sensitive systems.

F. *The Security Model*

In Fig. 3, you can find most of the drone's components discussed in the previous section.

The ground control station is the same as the ground base station, while the links shown represent the radio and GPS communication along with the satellite, which is the same as the communication infrastructure [15]. In addition, the drone's airframe combines the flight controller, accelerometers, gyros, magnetometers, pressure sensors, GPS, TV camera, and the payload controller as well.

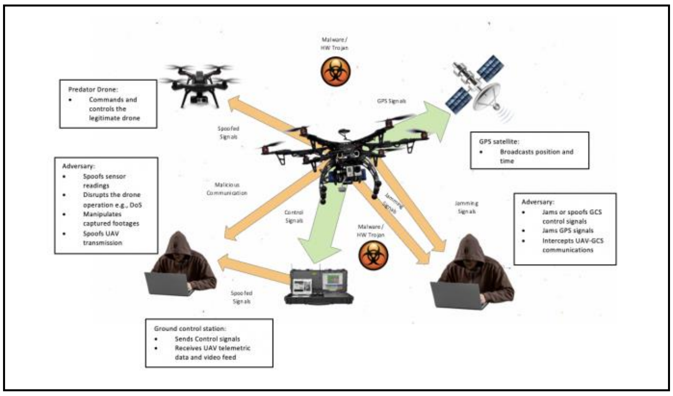
Malware / HW Trojan
Predator Drone:
• Commands and controls the legitimate drone
GPS Signals
Spoofed Signals
GPS satellite:
• Broadcasts position and time
Adversary:
• Spoofs sensor readings
• Disrupts the drone operation e.g., DoS
• Manipulates captured footages
• Spoofs UAV transmission
Malicious Communication
Control Signals
Jamming Signals
Malware / HW Trojan
Jamming Signals
Adversary:
• Jams or spoofs GCS control signals
• Jams GPS signals
• Intercepts UAV-GCS communications
Spoofed Signals
Ground control station:
• Sends Control signals
• Receives UAV telemetric data and video feed

Fig. 3. *Cyber-attacks, w.r.t. UAV components [15]*

G. Machine and Trust Boundaries

The boundary of a system is defined by the relationship which enables it to act as an interconnected and autonomous whole that reaches its limit. beyond that, the system is losing its control and must communicate with other systems and their environment. The previously mentioned components work together to achieve the drones' objectives as autonomous entities. The boundaries and security analysis related to each are discussed as follows:

- Start by the flight controller/computer as it collects a set of data from sensors like an accelerometer to control the drone’s speed, the pressure to control the drone’s height to an acceptable level, GPS module to guide the drone’s flight path, and other sensors to be analyzed by the flight controller and communicated with the ground base station and depending on that guides the actions on the drone. More specifically, the flight controller handles commands from the ground base station which in turn affects the actuators that have been deployed. Due to its important role, the flight controller can lead to serious effects if it is hacked or compromised as it may prevent communication with the ground base station or send false data and execute wrong decisions based on that. Also, GPS signals, which are not encrypted, can impose additional risks like spoofing attacks.
- Second, the drone airframe contains a set of payloads/sensors to monitor the physical environment like TV cameras sensors used to capture photos and video records and then send it to the flight controller or the ground base station for further analysis. Such sensors are controlled and monitored by the payload controller. The payload component is susceptible to being physically tampered with by malicious entities if the drones fall into their hands.
- The third boundary is the ground base station, GBS (Ground Base Station) is an on-land facility that provides human operators with the capability to track and/or control drones during their operations. It also communicates with the drone through a wireless connection to send instructions and receive real-time data. Once this component is compromised, it will put the whole drone’s system at risk as sensitive information can be accessed and wrong decisions can be made leading the drone to malfunction and break down.
- The fourth boundary to consider is the communication infrastructure shown between the drone and the ground base station. Drone missions are classified as per their distance from the GCS (Ground Control Station) into LOS (Line-of-Sight) missions where control signals can be transmitted and received via direct radio signals, and BLOS (Beyond line-of-sight) missions where the drone is operated by satellites or a relaying aircraft which can be a drone itself. However, these radio waves can impose risk as such waves can be spoofed easily or the communication channel can be jammed and thus blocked.

There are specific trust boundaries that need to be maintained in the drone’s system to ensure high security as it communicates with different components. For example, there is a trust boundary between the GBS and the flight controller such that the flight controller sends data and performs the instructions received from the GBS and considers any source of commands other than GBS as an untrusted source and thus ignores them. Another trust boundary must be maintained between GBS and the user who controls it such that any data entered by the user must be untrusted until the user signed with administrator account privilege.

H. Assets Mapping

Now, we will be mapping all the assets mentioned in chapter 1(domain analysis) to the components in the architecture that are discovered in this chapter

- Cameras(asset) are placed in the payload (the component in architecture)
- The GPS module (asset) is in the flight controller (the component in architecture and asset)
- The ESC (asset) is placed in the flight controller (a component in architecture and assets)
- Transmitter and Receiver (assets): they can be either in the flight controller or in the payload (components in architecture) according to what field they are in, this differs from one drone to another, it depends on the transmitter and receiver of each event), if they are related to the GPS, then they will be in the flight controller because the flight controller is the one that has the GPS module, but if they were related to cameras for an example, then they would be in the payload as it is the one that has cameras in it.

Now, we will discuss the relationship of the location of the asset in the architecture on the exploitation of the asset. The location of an asset in the drone architecture will affect the exploitation of the asset. For example, the GPS module which is a highly prioritized asset is embedded in the flight controller which is a very important component in the drone architecture and is considered as the core of the drone where it collects information from sensors and guides the drone to its path. Due to the importance of this component, it is considered as a target for all the attackers because of how much critical data it contains (it is also considered as an asset) and so that will raise the opportunity of the asset (ex. GPS module) being exploited.

All of the components of the architecture contain assets; each component has its specific assets that need to be protected. I think the flight controller holds too many assets (too much important information all in one place) which might impose a high risk on the drone if the flight controller is compromised and as a result, if the flight controller is compromised that will lead to high severe consequences because the compromise of the flight controller leads to the compromise of more than one asset at the same time.

Therefore in design analysis section we mainly focused on the architecture of the CPS drone's system, where we explained the architecture of the drone in detail by explaining all the components in the architecture and the flow of interaction of the components together, then we explained the security and some of the possible vulnerabilities that might be encountered in the different subsystems and the effect of compromising one of them on the system as a whole. After that, we discussed the communication of drones with external systems and the risks they might impose. Additionally, we elaborated on the possible evolution of drone architecture. Following that, we analyzed the security model of drones and identified the machine and trust boundaries of the system, and last but not least, we mapped the assets that we identified in section II (domain analysis) to the components of the architecture identified in this section.

IV. SECURITY ANALYSIS

In this chapter, we will be exploring and going deep into the details of drones by discovering their subdomains and the security concerns related to each subdomain. First, we will select three different drone subdomains and so we have chosen the GPS Module, the flight controller, and the communication wireless network, and then we will analyze the reason why we chose those three subdomains specifically. After that, we will perform a security analysis for each subdomain in order to discover the potential vulnerabilities and possible security risks that might appear in each subdomain. After that, we will provide a security concerns checklist to assist researchers in the future when they are referring to our case study for information. This will be achieved by providing them with a table that they can always refer back to which summarizes all the potential vulnerabilities and security concerns regarding drones in surveillance.

A. Selection of subdomains in survillance systems

In this section, three subdomains of drones have been chosen to conduct a security analysis. The subdomains are GPS module, Communication Network, and Flight Controller. The reason behind prefers these subdomains and give them higher importance is the critical functionalities they perform. Firstly we begin with, the GPS. Usually, an independent UAV relies on a GPS position sensor, providing highly accurate information that can be applied for control and surveillance purposes. To prevent accidents by other UAVs or manned vehicles, it is necessary to always know exactly where the drone is situated.

It is important to know the exact location of the drone when a measurement or photograph has been taken to accurately geographically reference the gathered data. The exact spot of the drone can be identified by a GPS receiver only. The accurate time and data note that UAV (GPS) gives are crucial in gathering this information, which reflects the importance of the security level in GPS. But despite his delicate tasks, he has a big vulnerability because the signals of GPS are unencrypted, which makes it spoofed easily by attackers and hijack the drone to get all collected data.

Finally communication network is considered as the most sensitive component because if it is compromised, many other assets will be affected. Also, the attackers always try to attack it because it is easy to break the communication between the ground base station and the controller. Finally, the Flight Controller is the brain of the drone just like the motherboard in computers. So, if it is attacked or compromised, most of the assets will be damaged since the flight controller communicates and is connected with many components and assets.

B. Security Analysis of subdomains in survillance systems

1) The GPS Module:

It is a satellite navigation system that collects signals from satellites in orbit using a radio receiver to determine the location, velocity and time. Consequently, the receiver sensor, which is an integrated part of drone's payload, is responsible for the drones navigation. It allows the drone to maintain the position at a specific place and altitude, knows the position it took off from, and automatically returns to this location at the click of the return home button and defines the drone's flight path by setting GPS waypoints which define the trajectory. The drone will then use autopilot to follow the direction upon operation. Civil GPS signals were built to be an open standard, available to all. There is a dangerous weakness in the clarity and predictability of its signals as they can be easily falsified or spoofed.

Civil GPS susceptibility to spoofing has significant consequences for civilian UAV since they have a comprehensive structure but no built-in fraud protection. For example, in the previously stated spoofing experiment (Shepard et al. 2012), an attacker received valid GPS signals in real-time, and spoofing signals were then generated based on the information obtained [27]. As a result, the drone lands on a position of its choice and thus will be hijacked by the attacker. Hijacking a drone leads to harm to all of the assets loaded on the drone's airframe. As a result, the payload includes all sensors (accelerometers, camera sensor, GPS receiver, etc.) and flight controllers will be compromised in return. The attacker can extract important data, like video records from camera sensors, and use it against the drone's owner.

However, an attacker should know the position, guidance, and waypoint of the target UAV and the status and internal signal processing method of the receiver installed at the UAV for spoofing which accurately leads UAV to a target point. On this basis, spoofing signals must be generated in such a way that they can have similar characteristics to those of legitimate GPS signals, and the spoofing signals produced must be radiated to the UAV at the correct signal strength.

A developer of the drone's internal signal processing algorithm can make the drone prone to spoofing attacks if no encryption is implemented for such a method. The company of civilian drones that use the civilian GPS system makes their produced drones prone to the spoofing attacks if they don't implement an encryption algorithm or cryptographic techniques to encrypt its GPS signals.

2) The Flight Controller

Its responsibility is demonstrated as it reads the sensor data, transforms it into useful information and then relays the information to the ground base station or supplies the actuator control units directly to the updated state, depending on the type of control. More specifically, the flight controller processes the command from the ground base station, GCS which in turn affects the actuators used. The flight controller incorporates multiple sensors onboard, or communicates with an outside sensor unit. So, if it is compromised, the onboard, the connected external sensors, the actuators, and the base station will be compromised in turn.

The flight controller's operation depends purely on the information obtained through the data link from the ground control station and collected from the surrounding environment by its sensors. Therefore, attacks on the flight controller without a data link with the ground base station are only possible if the intruder can access and control the internal system communication or produce the sensed physical properties in the environment. Since UAV operations depend almost entirely on multiple inputs from the external environment, most of the attacks begin with external malicious modification of these inputs [29].

Indeed, the flight controller is vulnerable to hardware and software trojans as shown in Fig. 2. These trojans can either be built or transferred discreetly to the system. An example of a virus infecting civilian drones is a Maldrone program which once installed on the drone, allows the attacker to take control of the UAV. To receive their instructions, the malware opens a backdoor link with its botmaster. Maldrone will then serve as a proxy for the flight controller and sensor interactions of the drone. In the flight controller chip, on the other hand, hardware trojans can be deliberately programmed to bypass those protection mechanisms and can have disastrous consequences when triggered. This is possible with the absence of physical-tamper resistance that must be provided by the company.

However, other vulnerabilities can be inherited by the flight controller from the vulnerabilities of the components/assets connected to it. For example, a drone's GPS receiver connected to the flight controller is known for its unencrypted signals leading to signal spoofing attacks. Additionally, sensors impose vulnerability by Injecting fabricated readings to the flight controller, thereby weakening the drone's secure control. It is possible to control all externally affected sensors such as radar, infrared and electro-optical sensors as the directed energy can be used to monitor the electromagnetic radiation and is not limited to radio and radar frequencies, but it also incorporates infrared, visible, and ultraviolet signals.

3) The Communication Wireless Network

Technically, all types of communication technologies can be used to control a UAV. The communication network is the part of drones that is responsible to transmit commands such as guiding and controlling payloads to the UAV flight controller and receiving flight sensor data and video or other data from the payload and sensors by the ground base station. As the communication network connects the flight controller with the base station and the user to transfer the data and commands, multiple assets will be affected in case of compromise. The attacker can send fake packets including a wrong decision to the flight controller and cause it to malfunction and thus harm the entire payload connected to it such as the accelerometers, the GPS module, and the pressure sensor. On the other hand, the attacker can falsify the packets sent to the ground base station exploiting vulnerabilities of a weak communication link.

For this role, different sources of electromagnetic radiation can be used. IR (Infrared) is the technology for communication used when there is a line of sight between the transmitter and the receiver and any obstacles between transmitter and receiver will interrupt the communication while radio waves are of longer wavelength electromagnetic radiation. Further, a uniform technology such as Wi-Fi or Bluetooth is used to control the communication of UAVs.

Going deeply into the communication technology used for the drone shown in Fig. 4, the visible telemetry link provides for more advanced control features, such as setting waypoints and automated flight. This is achieved from such a tablet running the flight control software which is connected to the telemetry box via Wi-Fi 802.11, which in return transmits the communication to the UAV using XBee 868LP chips.

The attacker needs to know the following communication parameters to communicate with an XBee 868LP chip: PAN ID (network ID), Baud rate, channel, DH (High Destination) address, and DL (Low Destination) address. However, The PAN ID, Baud rate, and channel for each UAV are all set to default values if the user did not change them. However, the XBee 868LP chips respond to broadcast packets sent within their network, hence the message of acknowledgment for the broadcast includes the sender's address, thereby exposing all available devices within the network. In addition, a security flaw was found in the Wi-Fi connection. The access point uses WEP (Wired Equivalent Privacy) as a secure communication protocol that has been discovered for its security weaknesses such as the absence of shared key management and other weaknesses in its security algorithms. It can, therefore, be hacked as users who use WEP fail to regularly change their keys. The hacker is able to break the password, disconnect the original user, and attach the UAV tablet to the attacker’s computer. But, for this to happen, the attacker must be within the range of the Wi-Fi link (100 m). In fact, if the user sets a weak Wi-Fi password, it will ease the job of the attacker to crack it." Commands Remote AT." feature allows the attacker to change the inner parameters of the XBee chips remotely, such as DH and DL, and thus reroute any traffic. Therefore, the company did not provide a protection mechanism against the remote command writing feature, and a new vulnerability is inherited in its communication components allowing for such man-in-the-middle attacks [25].

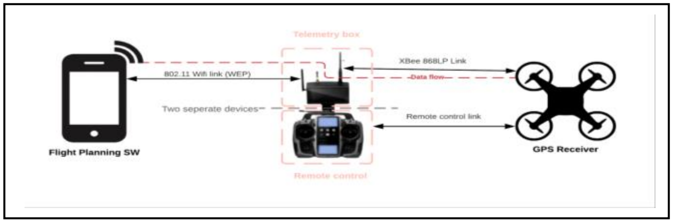

Fig. 4. *An example of UAV radio communication with XBEE 868LP and 802.11 Wi-Fi links. [25]*

C. Security Recommendations

Finally, we propose a recommended checklist for evaluating drones security in surveillance systems as a summary to the sections discussed in the paper.

TABLE II. SECURITY CONCERNS CHECKLIST

Security Concerns Checklist	
Domain-Specific Security Concerns	**Domain: CPS in drone surveillance** - Attacker's control over the drone's navigation system and as a result hijacking of the drone leads to the harm of all the assets loaded on the drone's airframe which is caused by GPS Spoofing attacks. - Malfunction of the GPS receiver in the UAV which is caused by GPS Jamming attacks - Crash of UAV and harm of the drone's system availability which is caused by Dos attacks - Access to the drone's system is caused by password theft (Authentication breach) . The password can be cracked by exploiting the weaknesses in the communication system and by conduction of dictionary attacks, brute force attacks, and statistical attacks. - Full control of the drone caused by the theft of the device - Access to (and ability to modify) confidential data without the knowledge of the attacked legitimate users which is caused by man in the middle attack (it can be conducted due to the weaknesses in the communication system, specifically the radio link, knowing the selected connection parameters can hack the link and that can be easily achieved as nearly all of them are still set to their default values, and are thus easy to search for.) - Having access to confidential data without the knowledge of the legitimate users of the drone is caused by eavesdropping.
Exclusive subdomain vulnerabilities	**Subdomain: Wi-Fi communication network** - WEP protocol does not have shared key management. - Using default or easy and uncomplicated Wi-Fi passwords that can be easily cracked. - unencrypted Wi-Fi is available and it also grants multiple users the ability to connect to the network
	Subdomain: Communication XBee chips The Communication XBee chips do not have the protection mechanism of remote commands executed in them.
	Subdomain: Flight controller - Vulnerable to trojans (Hardware +Software). - Vulnerable to injection of malicious data into sensors
	Subdomain: GPS Module - GPS Spoofing Attacks (original GPS-satellite-signals are overlaid by spoofed GPS-signals as GPS-signals are easy to spoof because they are not encrypted.) - GPS Jamming attacks The attacker produces signals in GPS jamming that conflict with the GPS signals, causing the GPS receiver in the UAV to malfunction.
Past vulnerability mistakes	Microdrones suffer from their high-power consumption and restricted power capacity.
Design concerns	Drones with longer wings tend to bump with obstacles more often.
	Fixed and rotary wings face crucial challenges in flying reliably when their sizes are minimized.
	Encryption techniques are not implemented in GPS modules of civilian drones.
Availability concerns	Denial Of Service attacks (scanning mid-air UAV ports to identify vulnerable or open ports in the network so they could exploit the vulnerabilities in the system.)

In the security analysis section, we have chosen three subdomains to conduct a security analysis to dig deeper into the subdomains of a drone and discover the vulnerabilities and security concerns available at each one. The three subdomains that we chose are the GPS module, the flight controller, and the communication wireless network. After conducting the security analysis on all the three different subdomains, we have come to find that the GPS module mainly suffers from spoofing attacks due to the fact that civilian GPS modules are unencrypted meaning that the GPS satellite signals are unencrypted. We have also concluded that most of the flight controller attacks begin from external malicious modifications of inputs because the UAV operations controlled by the flight controller depend almost entirely on multiple inputs from the external environment, and we have also found that flight controllers are vulnerable to hardware and software Trojans like Madrones. Eventually, for the communication wireless network, the security concerns come in the shape of fake packets including wrong decisions to flight controllers sent from attackers which causes flight controllers to malfunction and thus harm the entire payload connected to it such as the accelerometers, the GPS module, camera sensors, the pressure sensor, and many other sensors.

V. CONCLUSION

Drones are the most important component of any aerial surveillance systems. In this paper we investigated various aspects related to drone security. We tried our best to identify the important assets, their vulnerabilities and the threats mapping related to them. We conducted risk assessment based on the information gathered. We studied the architecture and design of the drones based surveillance systems and tried to make out the assets mapping and locations in the physical and logical proximities. Finally from them we selected the most important subdomains to make a thorough security analysis based on the related research works. Finally we propose a recommended security checklist, so that it can be a good reference for researchers interested in drone security. In future, we intend to exploit the published vulnerabilities and later conduct a vulnerability assessment and penetration testing (VAPT) on the drone based surveillance systems. This will let us address the unseen vulnerabilities in this area.

ACKNOWLEDGMENT

We thank in advance our anonymous reviewers for their feedback and comments, which will help us to further improve the quality of our paper.

REFERENCES

[1] E. Dahlman and K. Lagrelius, “A Game of Drones: Cyber Security in UAVs,”2016.http://www.divaportal.org/smash/get/diva2:1350857/FULLTEXT01.pdf

[2] “7 Different Uses for the Future of Drones,” Datafloq. [Online]. Available: https://datafloq.com/read/7-different-uses-for-the-future-of-drones/4936 . [Accessed: 17-Mar-2020].

[3] Admin, “5 Hour Endurance Hybrid Electric Drones for Surveillance and Mapping,” Skyfront, 19-Oct-2018. [Online]. Available: https://skyfront.com/ . [Accessed: 17-Mar-2020].

[4] O. Alhawi, M. Mustafa, and L. Cordeiro, “Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification,” Leuven, Belgium.https://www.esat.kuleuven.be/cosic/publications/article-3071.pdf

[5] AltiGator, “Electronic Speed Controller Maytech VESC60A,” Drones, UAV, OnyxStar, MikroKopter, ArduCopter, RPAS : AltiGator, drones, radio controlled aircrafts: aerial survey, inspection, video & photography. [Online]. Available: https://drones.altigator.com/electronic-speed-controller-maytech-vesc60a-p-42620.html . [Accessed: 17-Mar-2020].

[6] C. Bonilla, O. Parra, and J. Forero, “Common Security Attacks on Drones ,” International Journal of Applied Engineering Research ISSN 0973-4562, vol. 13, pp. 4982–4988 , 2018 .https://www.ripublication.com/ijaer18/ijaerv13n7_51.pdf

[7] C. Brook and C. Brook, “Many Commercial Drones 'Insecure by Design',” Threatpost English Global threatpost.com. [Online]. Available: https://threatpost.com/many-commercial-drones-insecure-by-design/125420/. [Accessed: 17-Mar-2020].

[8] “CERT/CC Vulnerability Note VU#334207,” VU#334207 - DBPOWER U818A WIFI quadcopter drone allows full filesystem permissions to anonymous FTP. [Online]. Available: https://www.kb.cert.org/vuls/id/334207/. [Accessed: 17-Mar-2020].

[9] DBPOWER U818A CVE-2017-3209 Security Bypass Vulnerability. [Online]. Available: https://www.securityfocus.com/bid/97564. [Accessed: 17-Mar-2020].

[10] K. Hartmann and C. Steup, “The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment,” Tallinn, Tallinn, 2013.

[11] “How Port Scanning Works,” Spam. [Online]. Available: https://www.spamlaws.com/how-port-scanning-works.html. [Accessed: 17-Mar-2020].

[12] “Matek F405 STD F4 BetaFlight Flight Controller,” Quadcopters.co.uk. [Online] . Available: https://www.quadcopters.co.uk/matek-f405-osd-f4-betaflight-flight-controller . [Accessed: 17-Mar-2020].

[13] “mkTR Camera Mount: Aerial photography, Camera, Photography,” Pinterest. [Online]. Available: https://www.pinterest.se/pin/342484746633538755/. [Accessed: 17-Mar-2020].

[14] “Vulnerability Details : CVE-2017-3209,” CVE. [Online]. Available: https://www.cvedetails.com/cve/CVE-2017-3209/. [Accessed: 17-Mar-2020].

[15] Altawy, R. and Youssef, A., 2016. Security, Privacy, and Safety Aspects of Civilian Drones. ACM Transactions on Cyber-Physical Systems, 1(2), pp.1-25.

[16] En.wikipedia.org. 2020. Trust Boundary. [online] Available at: <https://en.wikipedia.org/wiki/Trust_boundary > [Accessed 3 April 2020].

[17] Innovation, S., 2020. System Boundary - Systems Innovation. [online] Systems Innovation.Available at: <https://systemsinnovation.io/system-boundary/ > [Accessed 3 April 2020].

[18] Laksham, K., 2020. Unmanned Aerial Vehicle (Drones) In Public Health: A SWOT Analysis .https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6436288/

[19] Pastor, E., Lopez, J. and Royo, P., 2007. UAV Payload and Mission Control Hardware/Software Architecture. IEEE Aerospace and Electronic Systems Magazine, 22(6), pp.3-8.https://upcommons.upc.edu/bitstream/handle/2117/8697/25_digital%20_avionics_pastor.pdf

[20] Wang, L., Lai, C., Shuai, H., Lin, H., Li, C., Cheng, T. and Chen, C., 2019. Communications And Networking Technologies For Intelligent Drone Cruisers. [ebook] Available at: <https://arxiv.org/pdf/1910.05309.pdf > [Accessed 3 April 2020].

[21] Kaleem, Z. and Rehmani, M., 2018. Amateur Drone Monitoring: State-of-the-Art Architectures, Key Enabling Technologies, and Future Research Directions. IEEE Wireless Communications, 25(2), pp.150-159.https://arxiv.org/ftp/arxiv/papers/1710/1710.02382.pdf

[22] Kure, H., Islam, S. and Razzaque, M., 2018. An Integrated Cyber Security Risk Management Approach For A Cyber-Physical System. London.

[23] O. Alhawi, M. Mustafa and L. Cordiro, Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification. Manchester, 2020.

[24] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review", Progress in Aerospace Sciences, vol. 91, pp. 99-131, 2017. Available: https://www.researchgate.net/publication/316673697_Classifications_applications_and_design_challenges_of_drones_A_review .

[25] n. rodday, EXPLORING SECURITY VULNERABILITIES OF UNMANNED AERIAL VEHICLES. Amsterdam: DACS Research Group, 2015.

[26] "Understanding WEP Weaknesses - dummies", dummies, 2020. [Online]. Available: https://www.dummies.com/programming/networking/understanding-wep-weaknesses/ . [Accessed: 15- Apr- 2020].

[27] T. HUMPHREYS, STATEMENT ON THE VULNERABILITY OF CIVIL UNMANNED AERIAL VEHICLES AND OTHER SYSTEMS TO CIVIL GPS SPOOFING. AUSTIN, 2012.

[28] S. Seo, B. Lee, S. Im and G. 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. Available: https://www.researchgate.net/publication/283006977_Effect_of_Spoofing_on_Unmanned_Aerial_Vehicle_using_Counterfeited_GPS_Signal/link/56432a5a08ae451880a31f31/download.

[29] R. Altawy and A. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones", ACM Transactions on Cyber-Physical Systems, vol. 1, no. 2, pp. 1-25, 2017. Available: https://www.researchgate.net/publication/313329204_Security_Privacy_and_Safety_Aspects_of_Civilian_Drones_A_Survey.

[30] U. GPS, "UAV GPS Products – GPS UAV Receivers | TerrisGPS", TerrisGPS, 2020. [Online]. Available: http://www.terrisgps.com/how-is-gps-used-in-uav/ .[Accessed: 15- Apr- 2020].

[31] "buy drone parts - onlineshops.storecheap2021.com", Onlineshops.storecheap2021.com, 2021. [Online]. Available: https://onlineshops.storecheap2021.com/category?name=buy%20drone%20parts. [Accessed: 31- Dec- 2021].