Security models and exploitations in theory and practice for unmanned aerial vehicles

Martin Verup and Mikkel Olin

Kongens Lyngby 2016

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Richard Petersens Plads, building 324,
2800 Kongens Lyngby, Denmark
Phone +45 4525 3031
compute@compute.dtu.dk
www.compute.dtu.dk

Summary (English)

The goal of the thesis is to create a secure model for unmanned aerial vehicles with focus on both security, safety, and privacy aspects. To perform a risk analysis for a drone in its environment the ISO 27005 and CORAS tools are used to identify threats and vulnerabilities that, if left unattended, can be exploited, compromising security, safety or privacy. The thesis look at a couple of popular recreational drone models to evaluate and experiment on trying to find any vulnerabilities. Finally a model is created using the results from the analysis and is compared to real-life drone attacks. Evaluating the model against these attacks show that they could have been identified and prevented using this model, ensuring security for the drone system thus indirectly ensuring safety and privacy. To ensure safety and privacy more directly, the use of a dedicated drone legislation is needed.

Summary (Danish)

Målet med dette speciale er at skabe en sikkerhedsmodel for ubemandende flyvende fartøjer med fokus på både systemsikkerhed, fysisk sikkerhed og privatliv. Til at udføre en risikoanalyse for en drone i dens naturlige miljø er ISO 27005 og CORAS værktøjerne benyttet til at identificere trusler og sårbarheder, der, hvis der ikke sættes ind imod, kan blive udnyttet til at kompromittere både systemsikkerhed, fysisk sikkerhed og privatlivets fred. I dette speciale vil der blive kigget på nogle populære hobbydronermodeller og evaluere og eksperimentere på dem, for at forsøge at finde nogle sårbarheder. Til sidst, bliver der lavet en model, ved hjælp af resultaterne fra analysen og denne sammenlignes med virkelige droneangreb. Ved at evaluere modellen i forhold til disse angreb, ses det, at disse kunne være blevet identificeret og forhindret ved at bruge denne model og derved sikre systemsikkerhed for dronesystemet samt indirekte sikre fysisk sikkerhed og privatliv. For at sikre fysisk sikkerhed og privatliv mere direkte, er en specifik dronelovgivning nødvendig.

Preface

This thesis was prepared at DTU Compute in fulfilment of the requirements for acquiring an M.Sc. in Engineering.

The aim of the project is twofold as there is a theoretical and practical part.

The theoretical part is focusing on creating a security model of generic drones. To do this it is essential to understand the internals of how drones work, including:

- Understand the protocols used in drone communication.
- Identify drone positioning and navigation.
- Map out the sensor arrays and their applications.

From this analysis a security model including a threat- and attack model is created, which creates the basis of the practical part.

The practical part concerns working on one specific drone using the theory and models gained in the first part. During this part it is needed to:

- Identify and create a security evaluation including a model of vulnerabilities and exploits.
- Create a practical exploitation of an identified vulnerability.

Lyngby, 25-June-2016

Martin Verup Mikkel Olin

Martin Verup and Mikkel Olin

Acknowledgements

First of all we would like to thank our supervisor Christian Damsgaard Jensen for the continuous support, ideas and feedback throughout the entire thesis project period.

In addition we would like to thank our co-supervisor Michael Linden-Vørnle for proposals on how to approach the issues in the thesis and sharing his expertise in drones.

Finally we would like to thank Jakob Jakobsen for the opportunity to work in the DTU Space DroneCenter Lab and ideas on how to approach the drone experimentation.

Abbreviations

AES	Advanced Encryption Standard
AFHDS	Automatic Frequency Hopping Digital System
AHTD	Active Human Threat Deliberate
ARF	Almost-Ready-to-Fly
BNF	Bind-and-Fly
BVLOS	Beyond Visual Line of Sight
CIA	Confidentiality, Integrity and Availability
COTS	Commercial-Of-The-Shelf
ESC	Electronic Speed Control
GCM	Galois/Counter Mode
HTA	Human Threat Accidental
HTD	Human Threat Deliberate
IMU	Inertial Measurement Unit
ISR	Intelligence, Surveillance and Reconnaissance
NHT	Non-Human Threat
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PHTD	Passive Human Threat Deliberate

RPAS	Remotely Piloted Aircraft System
RPV	Remotely Piloted Vehicle
RTF	Ready-To-Fly
SDK	Software Development Kit
SDR	Software-Defined Radio
TCP	Transmission Control Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
VLOS	Visual Line of Sight

Contents

CHAPTER 1

Introduction

Unmanned aerial vehicles have existed for a long time. The technology today have made it possible to mass produce smaller and cheaper versions for use outside of the military. This opens up a whole new world of possibilities and practical applications for both industrial and public purposes. With this wave of cheap technology some concerns have come to light. Namely safety, security and privacy. To have a flying object that is a threat to its environment can become a big problem especially if the adaptation is continually rising. In this project we will take look at these flying drones to determine their role in both today's and tomorrow's society and map out practical uses and possible consequences identified through extensive risk- and threat analysis to create a thorough model of the typical drone, its components, information flows, to identify potential vulnerabilities and how to secure them.

Any vulnerabilities that could possibly be used the affect the navigation system and either take over control of the drone or get access to any payload. These could potentially be found in either the remote control communication or in the built-in sensors used to navigate autonomously. The goal is to create an extensive model of the drone and by including an attacker model and a risk assessment, map out all possible risks, consequences, and threats to both safety, security and privacy by looking at potential vulnerabilities or known exploitations. Finally a practical application of the theory from the security model will be executed to try and create a proof of concept that exploitation is possible and how it could have been identified using our secure model.

This thesis contains nine chapters:

In Chapter 1 a definition of a general drone and the different types of drones described.
Chapter 2 looks at the current and upcoming drone legislation in Denmark and it's relation to safety, security, and privacy.
Chapter 3 describes some of the different technologies available to be implemented and used in drones while also looking at the general drone model.
In Chapter 4, different risk management methodologies will be looked at and used to model threats and vulnerabilities in a drone system.
Chapter 5 uses the risk management from chapter 4 and create a risk assessment that identifies the different stakeholders, their assets and motivations for safety, security, and privacy.
Chapter 6 describes a few real-life test on vulnerabilities in drones, using WiFi based attacks and a Software-Defined Radio (SDR) to look at control signals.
In Chapter 7 a reflection on the risk assessment and experimentation will be described and used to give recommendations for a secure model for drones in general.
Chapter 8 reflects on the results from the model- recommendations and evaluation. Chapter 9 features concluding remarks and lessons learned during this project work.

1.1 Definition

How to define a drone? The term 'drone' is borrowed from insects living in colonies such as bees, ants etc. with the drones being all males. Roughly speaking they are expendable due to their huge quantity. For drones as a flying vehicle this is also true in some cases for instance when they are used in war scenarios.

Other names for drones used by more technologically oriented are Unmanned Aerial Vehicle (UAV) and Remotely Piloted Vehicle (RPV). In cases where several drones are linked together in a network it can be called Unmanned Aerial System (UAS) or Remotely Piloted Aircraft System (RPAS).

The definition for a drone, or rather UAV, is looked up in the Oxford Dictionaries webpage is as follows:

- *an aircraft piloted by remote control or onboard computers* [1]

This definition gives a good fundamental understanding of what a drone is and how it is controlled however in order for the drone to function interaction between several components is required. Generally speaking a drone is build up of the parts shown in Fig. 1.1.

[1] http://www.oxforddictionaries.com/definition/english/uav

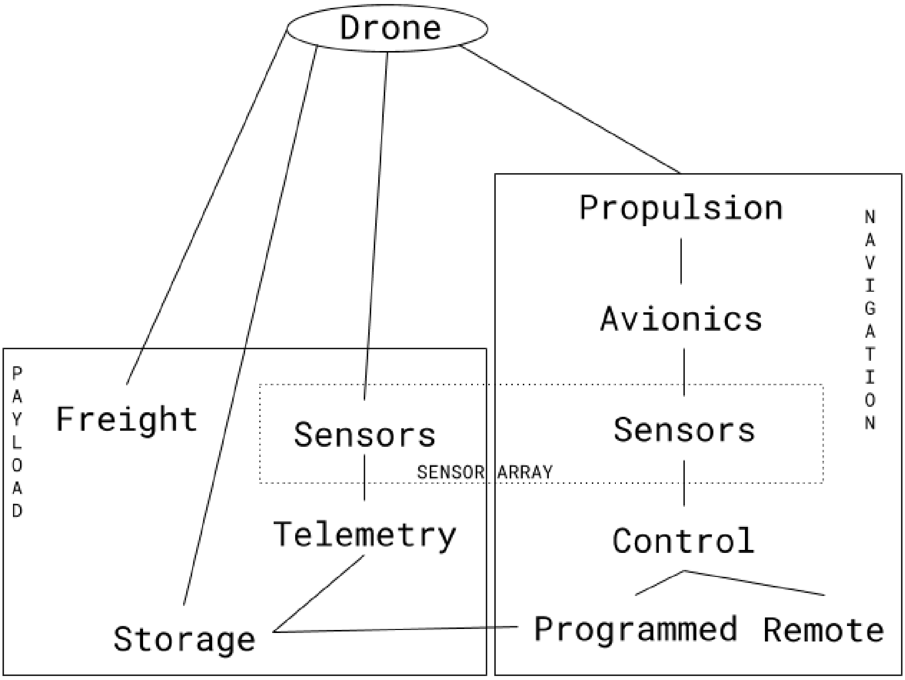


Figure 1.1: Model of a general drone system

Each of these parts each play an essential role in being able to get the drone to be working as intended, which basically is the ability to fly and communicate with the pilot:

Propulsion The mechanics keeping the drone airborne

Avionics System that controls the flying mechanisms

Sensors Sensors measuring various parameters used for either navigation or collection of data. Can often be the same sensors for both purposes

Remote Control Real time control by a pilot

Programmed Control Autonomous pre-programmed control

Freight Any objects that can be carried onboard

Telemetry Data send between the drone and the pilot or stored in the storage.

Storage An onboard storage containing data either telemetry data or pre-programmed control instructions.

As mentioned this description of a drone is general and the purpose of the drone is of great importance to which parts the drone consists of. The purpose of drones varies according to the field in which they are used. These fields are commonly known as:

- Military,
- Commercial, and
- Recreational

As one might think use of drones between the fields varies extensively

1.1.1 Military Drones

For decades drones have been used for surveillance and bombing raids in times of war. The reason this has mostly been to avoid losing pilots, but also in order to optimize the vehicle (or plane) in terms of weight, wind resistance fuel consumption etc..

The idea of using UAVs started during World War I with the development of the Kettering Bug in the US. The Kettering Bug was noting more than a flying torpedo in a wooden frame making it a predecessor for both UAVs and guided weapons such as cruise missiles. With a range up to 120 km it was able hit targets much further than any artillery at the time [1], but in order to do so it was required to calibrate each unit mechanically according to wind speed and direction. Even though about 50 units were ordered by the US military the war ended before they were used.

It was not until a few years before World War II that the idea was brought up again though it was for training anti aircraft personnel. The development of these UAVs was made by the company Radioplane who where ready with their first model RP-1 in 1935 [2]. The technology evolved during the following years and with the development of the RP-4 the US army chose to purchase the UAVs under the designation OQ-1. In 1939 the model OQ-2 was developed and due to World War II an estimated 15.000 units [2] were ordered by the US military making it the first mass produced drone. In Germany during World War II was late to use rather sophisticated drones in the form of the Vergeltungswaffe 1, better known as the V1 rocket, and its successor the V2 rocket. They both used the same principle of a mechanical 'autopilot' which included a magnetic compass and a gyroscope [3], even though the V2 autopilot was much more complex, to help guiding the missile to it destination.

Today the technology used in military UAVs are a lot more complex due to the development of the jet engine, computer etc.. As opposed to the early UAVs the modern models are controlled by an operator located in an airbase. The navigation is supported by a number of sensors in the drone such cameras and GPS which also makes it possible to order the drone to a specific location using auto-pilot. An example of these modern military drone is the RQ-1 Predator which were active in Iran and Afghanistan.

Sometimes it is not suitable however to use a drone at the size of a manned aircraft. For that reason the appearance of mini drones on the battlefield is increasing. One of the advantages of using mini drones is that they are able to fly into buildings to locate enemies. The PD-100 Black Hornet PRS [4] is such a mini drone. According to the company ProxDynamics who produce them the Black Hornet weighing 18 grams in total is able to fly 25 min with a maximum speed of 5 m/s (= 18 km/h) and contain a GPS and steerable camera.

1.1.2 Commercial Drones

In an investigation made by PwC in 2016 it was estimated that the total addressable value of drones in commercial context was $127,3 billion. In Table 1.1 is listed the values for each industry as estimated by PwC.

	2015
Infrastructure	45,2
Tranport	13,0
Insurance	6,8
Media & Entertainment	8,8
Telecommunication	6,3
Agriculture	32,4
Security	10,5
Mining	4,3
Total	**127,3**

Table 1.1: The value of drone powered solutions in all applicable industries in $ billion [5]

The obvious benefits of using drones is that they have a low response time and they are able to access areas which might be inaccessible to humans. This can be used in several fields to improve safety and quality of life as well as optimizing management of cities and the surrounding areas. As discussed by [6] there are several opportunities for drone integration by both the industry and by the public for use in cities.

Measure ground and sea levels:

A drone with a number of sensors can be used to fly over areas, take pictures and utilize other sensors to collect various information about a land- or sea mass. GIS surveying can potentially be done cheaper when using a drone over a pilot flying a plane over the same area. There are however still challenges to this. A research team have done experiments on this and even though they had difficulties with unstable image acquisition, they still conclude drones to be a much more flexible solution with more advantages than traditional methods, when studying river processes [7].

Inspection of constructions:

Once in a while constructions such as buildings and bridges needs to be inspected in order to locate damages. This can be done by using drones with cameras which can get to areas otherwise difficult to access.

Overview of accidents:

To get a quick overview of an accident the authorities could use drones. This will also help guiding the police and rescue teams before they arrive at the accident.

Defibrillator transport:

The initiative of placing easily accessible defibrillators in populated areas has been around for years, but it is not always the case that there is a defibrillator within reasonable range. Using drones as transportation device the help can get to any location within minutes [8] by contacting the emergency hotline with an app which send the coordinates where the defibrillator is needed.

Civil Security Control:

Drones could be used to help the police or national guard in cases such as demonstrations, man hunts etc.. The advantage of using drones is that there are multiple eyes in the sky instead of a handful of helicopters.

Natural Disaster Control and Monitoring:

At times it is difficult to enter areas affected by natural disasters. Therefore it makes sense to send drones in the area to locate survivors or possible routes into the area. In case of injured persons the drones could also carry emergency aid packages.

Agriculture Management and Surveillance:

Using drones in agriculture can help with spreading fertilizer over a vast area. Using cameras attached to drones it is also possible to keep an eye on the crops and estimate the harvest.

Environmental Surveillance:

Attaching air sensors to drones they could be used survey areas where there is a possibility for leaks such as oil and gas refineries. In addition they could be used in cities to monitor the level of exhaust gases.

Traffic Management:

With the increasing world population and thereby increasing number of transportation vehicles (such as cars) become a problem in relation to transportation time. By using drone to monitor the traffic flow during for instance rush hour the traffic can be guided in order to optimize the flow allowing the drivers to get to their destination faster.

1.1.3 Recreational Drones

For recreational use there exist three main types of drones [9]:

Ready-To-Fly (RTF)

Also known a Commercial-Of-The-Shelf (COTS) drones, this type is ready to be used as soon as the owner has charged it. This type of drones are mostly "toy" drones with none or few sensors and limited fly-time. To fly the the drone a dedicated controller is needed.

Bind-and-Fly (BNF)

These drones does not have a dedicated controller and are instead controlled by binding a device (smartphone, tablet, etc.) to the drone. This also gives more possibilities for the use of sensors.

Almost-Ready-to-Fly (ARF)

This type of drone is assembled by the user and therefore requires extended knowledge of the underlying technology. The number of sensors on the drone is only limited by their energy consumption and weight.

In a lot of cases, specially for BNF and ARF, the drone will have a camera attached to allow video recording and taking pictures from a perspective not possible before. Taking photos and videos from angles not easily accessible is fun for hobbyist and a new opportunity for professional photographers.

This however raises a big privacy concern as it opens up the possibility to look into windows high above ground or without being on the property of the building as well as more discretely spying on other people.

Additionally there the whole issue about the drone itself and the safety about it flying around in the sky. Consequences of what could happen if it were to fall down and hit something or just it's presence in the airspace in unwanted places are just a few of the many concerns this rising trend is imposing on today's and tomorrow's society. Another perspective to consider is the that the cheap mass produced drones probably aren't properly secured which opens up the possibility for exploitation.

To ensure the public interest of safety and privacy some legislation is in place for use of drones. The legislation is an important part in how to deal with these issues.

Chapter 2

Drone legislation in Denmark

Before drones were introduced on the Danish market for recreational and commercial purposes there already existed provisions called Regulations for Civil Aviation BL 9-4 last modified January 9. 2004. These regulations addresses unmanned aircrafts below 25 kg and establishes 7 general provisions:

a. The flight must be performed in such a way that lives and property are not endangered, and so that the environment is applied as little inconvenience as possible.

b. The distance to the course / courses at a public airfield as indicated on National Survey and Cadastre maps must be at least 5 km.

c. The distance to the course / courses at a military airbase as indicated on the National Survey and Cadastre maps must be at least 8 km.

d. The distance to urban areas and greater public roads must be at least 150 metre.

e. The flight altitude must not exceed 100 m above ground.

f. Densely populated areas, including holiday home areas and inhabited camping sites, as well as areas where a greater number of people are gathered in the open air shall not be overflown.

g. The particularly sensitive natural areas mentioned in BL 7-16 shall not be overflown.

which concerns aircrafts below 7 kg. If the aircraft is above 7 kg then there are 4 special provisions which must also be met:

a. The aircraft must be equipped with radio control equipment.

b. Flights shall only be made from an approved model airfield and must take place within the limits of the airspace to a notified model airfield.

c. Flights must not take place unless there is liability insurance in accordance wit the Danish Aviation Act.

d. The flight must be conducted under an organization approved by the State Aviation Administration, which is designed to operate flights with model aircraft amateur basis and in accordance with regulations approved by Civil Aviation Administration.

Even though the Regulations for Civil Aviation BL 9-4

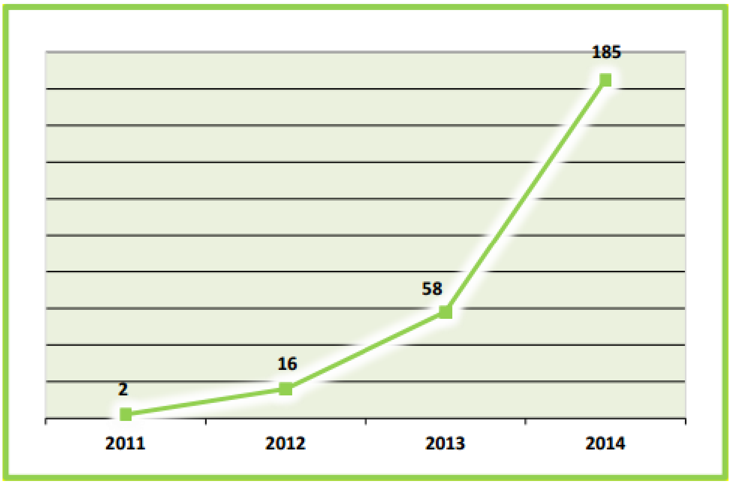


Figure 2.1: The number of cases reported to the Danish Transport Authority each year relating to drones [10]

As the graph show the number of reported incidents involving drones has been increasing in the period 2011 to 2014 and it is expected to keep increasing in the coming years [10]. Even though it is not clarified what kind incidents the drones have been involved in it is thought that flying over populated areas and flying near airports has been the main cause for the reports.

2.1 Proposed Danish drone legislation

To counter the increasing number of incident an inter-ministerial working-group consisting of:

- The Ministry of Justice including
  - the Danish Security and Intelligence Service (PET)
  - the Danish National Police
- The Ministry of Business and Growth represented by

    - the Danish Business Authority
- The Ministry of Defence represented by
    - the Danish Defence Intelligence Service
    - the Danish Defence Acquisition and Logistics Organisation
- The Ministry of Transport

was formed to come up with recommendations for a new drone legislation. The result was a report published in March 2015 with focus on drones weighing less than 25 kg and flying below 150 m.

The working-group recommend that the existing provisions in BL 9-4 should be retained but also that it is necessary to introduce some modifications and additional regulations, including a triviality threshold and a drone register.

For drones having a weight of at most 250 g the triviality threshold should be introduced as they are not considered to be a threat to the safety of the citizens by the working-group. Drones weighing more than 250 g a 'driving' license should be acquired in order to legally operate them.

Creation of a register should initially involve all professional drones, giving them a drone 'number plate'[1] , and issued driving 'licenses'. Later on the 'number plate' registration should also be applied to the recreational drones.

The table below sums up the recommendations put forth by the working groups

[1] Expression used in [10] page 8, Box 1.

	Permission	ID	GPS Logging	Liability Insurance	Training Reqs	Airworthiness / Technical Reqs
Up to 250 g without camera or similar device						
Up to 250 g with camera or similar device		X				
Recreational						
0.250 kg to 1.5 kg		X		X	Drone permit	
1.5 kg to 7 kg		X		X	Drone permit	
7 kg to 25 kg		X		X	Drone permit	
Commercial & Emergency Response						
Up to 250 g without camera or similar device						
Up to 250 g with camera or similar device		X				
0.250 kg to 1.5 kg	X	X		X	Drone License A	
1.5 kg to 7 kg	X	X	X	X	Drone License B	
7 kg to 25 kg	X	X	X	X	Drone License C	
BVLOS up to 2.5 kg	X	X	X	X	Drone License D	X
>25 kg	X	X	X	X	Case by case basis	X

Table 2.1: The recommended framework for regulation of recreational, commercial and emergency response drones [10].

Permission A permission is needed for companies if they wish to use a drone in a populated area. To get such a permission the drone must be identifiable and the operation must be logged in case of future accusations of misuses.

ID The identification of a drone is transmitted through a radio signal which can be picked up by the authorities. It is expected that the signal will contain the name, address and phone number of the owner. If the drone weighs below

250 g and has no camera then it would not be required.

GPS Logging All drones used in commercial or emergency response context should be tracked using GPS logging. The main reason is 'to safeguard citizens and for use as documentation in connection with complaints, accidents, etc.' [10].

Liability Insurance At the moment only professional drone users are obliged to acquire a third-party liability insurance. However the working-group has the opinion that all drone users who owns a drone above 250 g should be obliged to acquire an insurance.

In BL 9-4 only professional users of UAVs were instructed to acquire a third-party liability insurance. However, since family insurance policies does not cover the recreational use of drones the working-group recommend introducing liability insurance for all users of drones.

Training Requirements The training required for an operator is dependent on the category in which he/she is going to operate a drone in. For recreational purposes the operator only needs to acquire a drone permit (also known as a drone 'driving' license). The operators for commercial or emergency response drones is obliged to acquire a drone license in the range A to D depending on the weight of the drone.

Airworthiness / Technical Requirements For professional users the level of airworthiness of the drone needs to be documented and approved by the authorities before the drone is able to fly. In addition the drone should fulfill some technical requirements which as a first instance should include electronic 'number plates' and lights. In time the requirement could be extended to meet future needs.

2.2 Adopted Danish drone legislation

The Danish Minister of Transport and Construction, Hans Christian Schmidt has stated that:

> *We take the necessary respect to safety and privacy, so that the citizens can feel safe as the industry and technology evolves* [11]

As such the recommendations are not followed with respect to a triviality threshold and special requirements only for professional drone pilots. Instead the it is required that all drone pilot, including those who have a recreational drone, acquire a drone 'license', an insurance and registration of the drone. In a consultation letter send out by the Danish Transportation and Construction Agency on June 8. [12] the proposed new legislation is summarised. The letter lists the requirements that must be met before, during and after the flight for drones weighing less than 25 kg flying in a populated area.

Requirements before flight:

- Registration and labeling of drone
- Insurance
- Age limit of 18 years
- Drone 'license'
- Experience
- Creating flight and safety area
- Obtaining information on airspace

- Obtaining special permits for flights with elevated flight safety risk
- Orientation of residents and obtaining other licenses

Requirements during flight:

- The drone and drone system
- Monitoring of airspace
- Right of way rules
- Flight altitudes and distances

Requirements after flight:

- Imports into the logbook of flight information

In the original decree on flight with drones in populated areas the punishment for violating the provision set out to fines unless another penalty is prescribed [13]. As such the pilot can only be ordered to pay a fine or more depending on the violation extent unless any aviation laws are being violated.

Chapter 3

Technologies in UAV's

As drone is widely specific term, creating a model of the internal design and mapping the technologies of one is not that simple. There is, however, a minimal set of requirements in order to make a drone airborne, keeping it steady in air and to control it from a ground control. In Fig. 3.1 a model of a drone in its general form has been created to better understand the internal works, the data flow and to specify the specific technologies used both internally and externally.

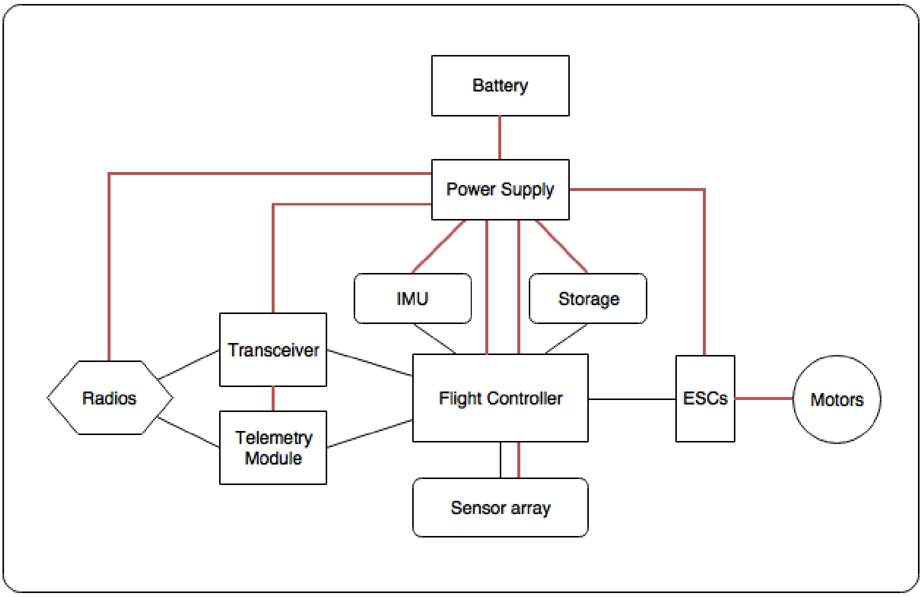


Figure 3.1: Model of components in a drone

Battery The power source feeding power to all the components.

ESC Electronic Speed Control. Adjusts the power going to the motors based on data from the IMU to keep the drone steady in air. One for each motor: 4 in a quadcopter, 6 in a hexacopter etc.

Flight Controller The main component responsible for calculating and relaying sensor data to both the telemetry module, ESCs and on-board storage.

IMU Inertial Measurement Unit. Collection of sensors, typically gyroscope and accelerometer but sometimes also magnetometer and GPS. Measures aviation specific data such as g-force, angular rate and sometimes actual position.

Motor Purpose of spinning propellers to create propulsion making the drone airborne.

Power Supply Ensures the correct amount of power goes to the components.

Radio Transmits and receives radio waves used for navigation by remote control and to supply telemetry data.

Sensor Array Collection of additional sensors, either used for navigation or data collection - sometimes both. Can be sensors such as altimeter, proximity sensor or a camera.

Storage On-board storage to store sensor specific data.

Telemetry Module Collects sensor data in real-time and transmit back to the ground control.

Transceiver Deals with radio signals received and data to be transmitted. Responsible for data processing such as compression, digital/analog conversion and modulation.

3.1 Wireless Remote Control

If a drone is not autonomous it must be remotely controlled somewhere. This means that there's some wireless communication going to the drone from the ground control using a remote. Often there will also be some communication going the other way, typically a video feed. To transfer data back and forth the devices needs to establish a connection, usually done with a handshake. How the handshake works differ from protocol to protocol but some of the most known are the 3-way- and the 4-way handshake used by the TCP and WPA protocols respectively. There exists numerous protocols for wireless communication, however in case of drones it isn't just a pick and chose scenario. Drones often have very limited computational power, limited power supply but need to communicate at a reasonable distance preferably without line of sight while still be able to communicate in real time.

3.1.1 Communication Protocols

Using radio waves for wireless communication is the standard today. The frequencies of radio waves span from 3 kHz to 300 GHz but a lot of these are restricted and requires permission to use. There are however some frequencies open for free use which are obvious choices to use. These frequencies are called the Industrial, Scientific and Medical bands, or ISM bands. Some of these frequencies are [10, Section 6.1]

- 27/35/40 MHz
- 433 MHz
- 2.4 GHz
- 5 GHz

There exists more open frequencies, both higher and lower but these are generally not used or considered outside special cases and not viable in devices such as consumer electronics. Each of these frequencies have their own advantages and disadvantages. Lower frequencies have better penetration power but requires longer antennas and can carry less data, while the higher frequencies are more easily obstructed than the lower frequencies, can carry more data but consumes more power. Some regional restrictions are also in place where some frequencies are open in some places of the world while not in others. Manufactures will have to take this into account depending on where they want to sell their RF devices.

	Region 1	**Region 2**	**Region 3**
27/35/40 MHz	✓	✓	✓
433 MHz	✓	✗	✗
915 MHz	✗	✓	✗
2.4 GHz	✓	✓	✓
5 GHz	✓	✓	✓

Table 3.1: The ISM bands and regions

Generally the ITU regions can be described as follows. Region 1 is Europe and Africa, Region 2 the Americas and Region 3 Asia and Australia. This is important to take into account as a device using the 433 MHz frequency can be sold within Europe but not in the USA, while the opposite is true for the 915 MHz frequency.

WiFi IEEE 802.11
Choosing WiFi is an obvious choice. WiFi is proven standard and is found in over 10 billion devices in the world [14]. WiFi typically operates on the free 2.4 GHz frequency but also 5 GHz have been gaining ground. The strength of WiFi is that it is a proven, reliable protocol already implemented in most mobile devices. WiFi however have the disadvantage of a relatively high power consumption [15] which decreases the battery life significantly in an already lightweight device. The data rate is however high enough to transmit a live video feed in uncompressed form back to the device.

Bluetooth IEEE 802.15.1
Bluetooth also operates on the 2.4 GHz frequency and with version 4 and upwards offers significant low power usage. Especially compared to WiFi. The range is however a limiting factor thus making Bluetooth only usable to communicate over short distances. The longest range for Bluetooth is Class 1 with a range of 100 meter. The low data rate of Bluetooth compared to WiFi is however the biggest bottleneck. Bluetooth 2.0 have a data rate of only 3 MBps and Bluetooth 4.0 at 24 MBps which is not sufficient for a video stream back to the device.

RF A generic term for all communication with radio frequencies. Other IEEE standards exists for wireless communication, e.g. IEEE 802.15.4 ZigBee that have a really low power consumption but a data rate so low that it isn't feasible for most drones. As more bandwidth and range requires more power it really is a trade off the manufacturer has to deal with. Looking at the currently most popular recreational drones seen in Fig. A.1, it seems that most have settled on using 2.4 GHz as evident in Table A.1. The drawback on this frequency is that is often will require a line of sight as higher frequencies struggle to penetrate objects such as buildings. Also there's the risk of interference from other devices using the same frequency. At the 2012 World Radiocommunication Conferences the member countries agreed to reserve the 5030-5091 MHz frequencies for internationally standardised aeronautical systems including recreational drones [10, Section 6.5]. It appears that most manufactures are settled on using the 2.4 GHz frequency even though that this frequency is heavily used by a lot of devices as this is an ISM band. One way to limit the interference of other devices can be by using what is called frequency hopping. As thr 2.4GHz is more of a range than a very specific frenquency it has been divided into different channels with each their own little varying frequency. By detecting if a channel is used by other devices frequency hopping can be used to switch to another channel without as much interference.

3.2 Sensors

The number of sensors which can be put on an UAV is limited by the size and price range. The cheapest of them available for everyday people may only have a camera or maybe no sensors at all. This also restrict the use of the UAV to within the visual range of the operator. Since the range of the application of UAVs is nearly unlimited the number of sensors available is too. Sensors can be divided into two categories: Navigational or Data collecting. The navigational sensors are used to ease the controlling of the drone either for the operator or the auto pilot. The data collecting sensors on the other hand are only used to gather information which are send to the operator or stored until the drone return to the operator.

3.2.1 Navigation sensors

In order to use sensors to navigate a drone it is essential to maintain a communication channel between the operator and the drone. Alternatively using an auto pilot this is not required but it is comforting to get the navigation data all the same to make sure that the drone is functioning.

Camera Most UAVs are equipped with some kind of camera no matter the application. This is because the camera can be used to control the UAV by a real time video link. Otherwise the camera can be used to take photographic images.

GPS Short for Global Positioning System this sensor is used to identify the geological position of the drone. To do this the GPS makes contact with several satellites orbiting Earth.

Proximity sensor A relatively new technology (in private drones) the proximity sensor measures the distance to surrounding objects. The flight path can then be corrected to prevent collision with the objects and damaging the drone.

Thermal sensor The application of thermal sensors are mostly for vehicles operated during nighttime to detect warm objects or people.

Magnetometer An electronic form of a compass this sensor is able to measure the direction of magnetic fields such as the magnetic field of the Earth. This makes it usable for cross-referencing with GPS information.

Accelerometer The G-force working on the drone can be detected by an accelerometer.

Gyro Sensor In case the drone begin to rotate about its own axis a gyro sensor is able to detect it. The rotation might be the result from a failure or damage to the drone and can give the operator an idea whether the drone is fit for service or not.

Altimeter This sensor measures the altitude of the drone

Ultrasound An ultrasound or ultrasonic sensor can be used to measure the distance to objects or the ground in order to maintain a certain altitude.

3.2.2 Data collecting sensors

As mentioned the data collecting can be done in two ways:

1. send the data directly to the operator or
2. save the data on some storage device in the drone.

Air quality sensor The ability to measure the air quality in different heights in the atmosphere. The sensor can for instance be used to measure CO, CO_2

or O_3 in an area giving the information required to make precautions for the population.

Hyperspectral sensor A hyperspectral sensor works like a camera but is able to process information from a wide range in the electromagnetic spectrum. This makes it useful for detecting areas or objects which may be difficult to identify on an ordinary photography.

LIDAR As an alternative to take pictures one can use a LIDAR which can make 3D models of objects or areas by using a laser.

Electro-optical Sensor A light sensor that detects the presence or absence of light to act accordingly such as turning on light when its dark.

Photoelectric sensor Using light, often infrared, to determine the presence or absence of an object but also distance of that object.

With all of these sophisticated technologies - sensors and wireless protocols - the overall drone system becomes susceptible to the same vulnerabilities as the individual components. The system is not more secure than the weakest link. As such, it is of utmost importance to identify any possible vulnerabilities and create a thorough risk analysis to limit the possibility of exploitation.

Chapter 4

Risk Management

As drones are becoming more mainstream the safety, security, and privacy aspect are more relevant than ever. If security measures are not properly implemented, drones are now a bigger risk for both safety and privacy. As the sheer volume of drones are rising so are the associated risk imposed by various vulnerabilities. No system is free of vulnerabilities but if no effort are done in order to minimize them the threats to our safety and privacy might become a rising problem in our society. There have already been drone incidents that has affected safety[16], security[17] and privacy[18].

For private drones data can be differentiated by control data and information data [19]. The control data is the data used for navigational parts of the drone, while the information data contains the state of the drone and is also called telemetry data.

In order to make a risk management it is important to understand the drone and its surroundings. An example of such is shown on Fig. 4.1 containing:

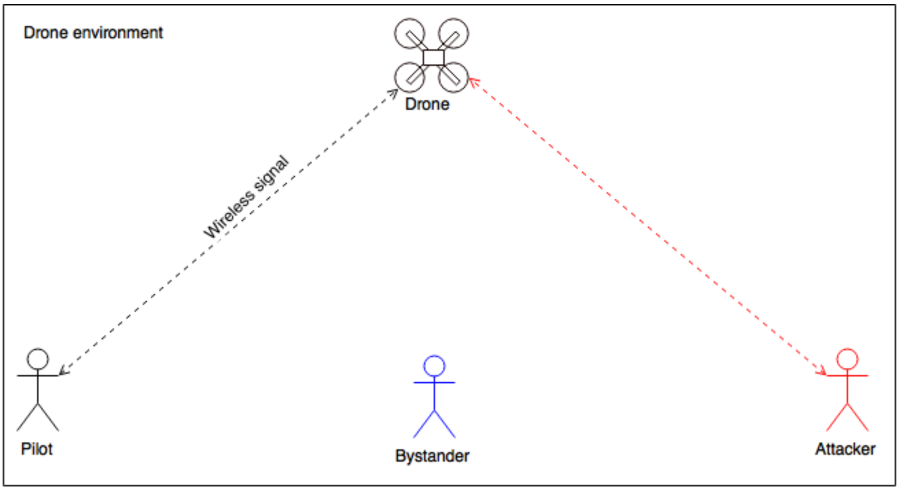


Figure 4.1: An example of a drone environment containing a drone, pilot, attacker and bystander.

Drone environment The area within the flying radius of the drone.

Drone The UAV controlled by the pilot or the attacker.

Pilot The person in control of the drone unless it is taken over by the attacker.

Attacker A malicious person who tries to attack the drone logically.

Bystander Any person in the drone environment who are not the pilot or the attacker.

These definitions will be used without the rest of this thesis.

4.1 Security, Safety, and Privacy

Most of the time when a system is analysed within the field of information technology the only interesting matter is to ensure security. This is however not true for a drone environment since a four party is included; the bystanders. For them the security of the drone is of no interest unless it leads to a violation of safety or privacy. For that reason it is equally important to talk about safety and privacy when talking about drone risk management.

Security

When we talk about information security there are 3 primary properties that need to be addressed before we call a system secure. The 3 properties are *Confidentiality*, *Integrity* and *Availability*, also known by its short form *CIA*. In addition we would like to add safety and privacy. But more properties which are also often desired exists and also needs to be addressed in order to maximize the security of a system.

Confidentiality Ensuring the message can only be read by the rightful sender and recipient. Usually done by encrypting the message.

Integrity Ensuring the message has not been altered on its way from sender to recipient. Usually done by comparing checksums by hashing the message on both ends.

Availability Ensuring the message can reach its destination. If the recipient never receives the message either because the system is too heavily guarded by other security measures or it is vulnerable to interference or denial-of-service attacks, the system is no good. Usually availability can be hard to protect against but there exists methods such as changing communication channels.

Authenticity Ensuring authentication is to be sure that the message is really from the acclaimed sender. Usually done by having a shared secret that can be hashed and sent. If the recipient can recreate the same hash, the sender must be valid.

Safety

The term safety in the drone environment means to protect the environment against the drone in a physical sense. This include both human safety as well as safety for any property which might be within the environment. In addition the safety of the drone should be considered since drones are highly movable vehicles able to do damage to itself in collision with the ground or walls in the environment.

Privacy

As with safety privacy is a matter of protecting the environment from the drone but in different way as privacy is a matter of information gathering without the consent of the affected people. The compromise of privacy will usually be seen as spying, but the purpose can be varying from reconnaissance for a break-in to sneak peeking on the neighbour for fun.

4.2 Origins of Attacks

To properly understand what to prevent and protect against it is important to know where the attacks might come from. Who wants to attack the system and what is their motivation for doing so. Understanding this is a crucial step in discovering any likely attack vectors, their impact and likelihood.

4.2.1 Attackers

There exist several kinds of attackers which are determined by the amount of resources available and the motive. Of course the level of experience is also a vital part, but it is not the dominant factor in attacker determination for most of the attackers.

Script kiddies

The lowest kind of attacker in terms of both resources and mostly also experience. The reason for them to do the attacks are basic since they want to impress their friends or simply because they are able to do the attack.

Hackers

The challenge and/or the fame which may follows are what the plain hacker strives for. In addition the experience gained from doing the attack may also be a reason for do it.

Criminals

In recent year the number of cases involving computer criminals have been increasing and it often turns out that it is on a organized level. The only goal for them is to gain money from their victims by using methods such as phishing or blackmailing.

Insiders

Contacted by third parties they hand over information or search for information in the organization in exchange for money. Otherwise they could do it on their own initiative to do damage to the organisation.

Spies

The use of spies to gain knowledge of your enemies and competitors have always existed. Today however the means to get the information is also involve getting access to their systems since most modern organizations make use of some kind of electronic storage device linked up to their computer network.

Terrorists

The main goal for terrorist are to spread terror using their ideological believes as the argument to do so. The attacks are meant to be publicly known otherwise it would be nearly as effective as intended. Alternatively the terrorists could try to get information which can be used in attacks.

Activist

Hacking activists, or hacktivists for short, are hackers who has an interest to spread a message, gain information or do harm to organizations that the hacktivists are convinced have done something illegal either in the context of law or ethics.

All attackers must be accounted for in order to produce a secure an thorough risk analysis, however some may be more relevant than others. In regards to drones, the biggest concern is evaluated be terrorists and spies.

4.2.1.1 Abusers

An attack on safety and privacy might not come from an attacker. The motivation of the pilot can be just as malicious as an attackers. The pilot could be interested in filming inside other peoples windows, violating their privacy, or fly over restricted areas, for example airfields or company buildings to gather intelligence on an area. Drones can also be used to transport items, for example to smuggle drugs or other contraband inside prisons. These kinds of abusers often have a criminal motive.

Other abusers can be thoughtless people that have no regards to other people's or property safety. This is often the cause of insufficient training.

Safety and privacy violations from an abusing pilot and not attackers are difficult to prevent. The best way is probably to deter this behaviour by a special drone legislation.

4.2.2 Types of attacks

Attacks may come from anywhere and in any form. All attackers have different motivation for doing what they do and each have a purpose.

When attacking the network communication it can happen in multiple ways, each method with a different purpose. These attacks are all man-in-the-middle attacks.

Deletion

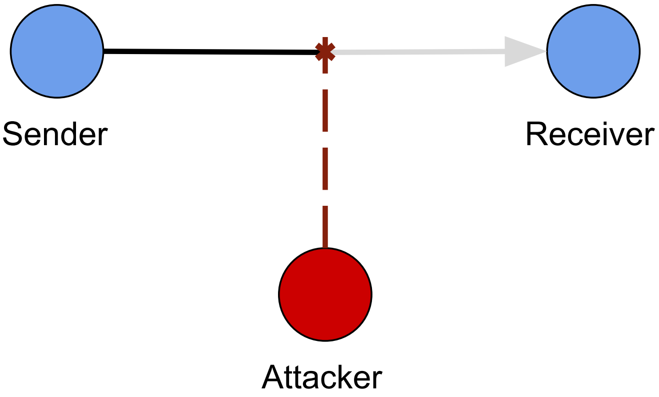


Figure 4.2: Basic concept of a deletion attack

Simply deleting the network packets will prevent the recipient from ever receiving anything and unaware that anything was tried to be sent.

The availability is violated.

Drone example: This attack could prevent remote control as the packets would never reach it.

Fabrication

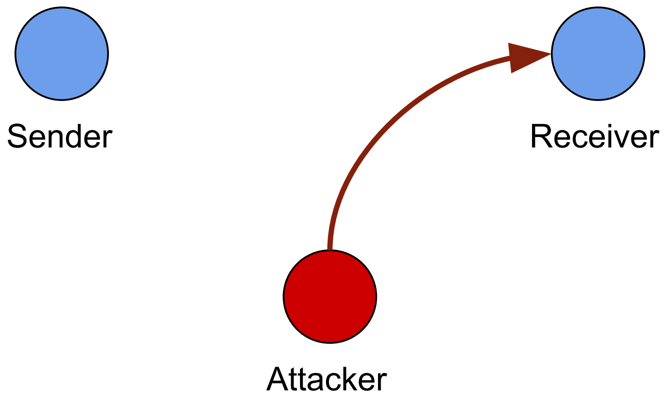


Figure 4.3: Basic concept of a fabrication attack

Creating new fake network packets and sending them to a recipient can make them act as they received legitimate packets from someone else, someone they trust.

The authentication is violated.

Drone example: This attack could allow someone otherwise unauthorized to take control over it.

Modification

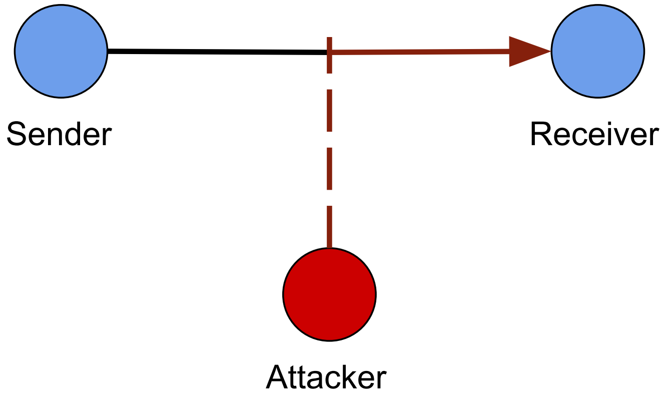


Figure 4.4: Basic concept of a modification attack

Modifying a packet sent to the recipient could allow an attacker to alter the data received and could result in unexpected behaviour from the sender.

The integrity is violated.

Drone example: This attack could allow someone to hijack the control so the operator's commands are misinterpreted by the drone resulting the drone in being uncontrollable.

Eavesdropping

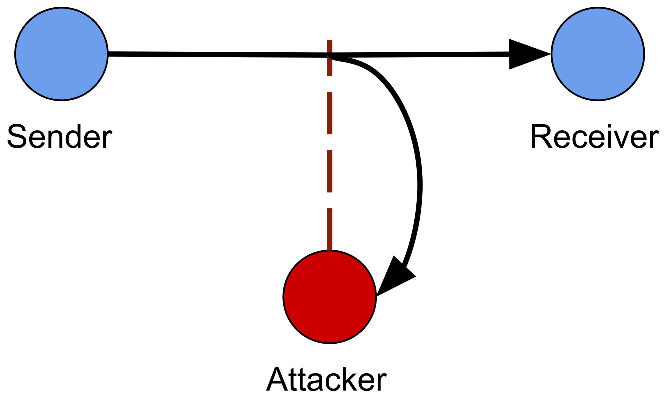


Figure 4.5: Basic concept of an eavesdropping attack

Eavesdropping is a passive attack that may let the eavesdropper learn how packets are crafted in order to later perform one the active attacks mentioned above or to simply get a copy of the data.
The confidentiality is violated.
Drone example: This could allow an attacker to learn how the drone specific packets are crafted and use that knowledge later in an active attack.

Traffic analysis

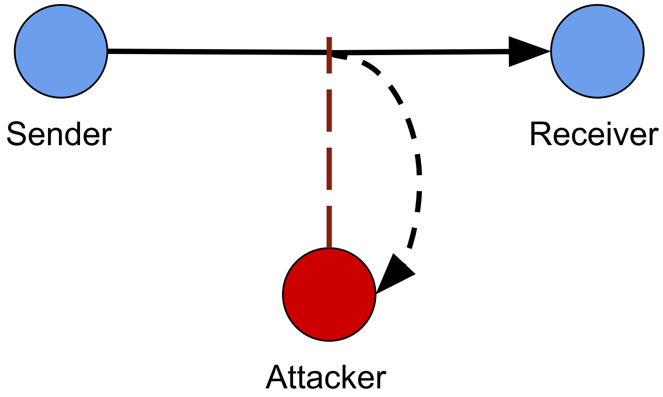


Figure 4.6: Traffic Analysis

Traffic analysis is a passive attack that collects meta data in order to reveal specific patterns about the communication. It can be all sorts of things such as how commands look, frequency of communication, size of packets etc.

Traffic analysis is not really a violation of any of the CIA properties but a method to gather information that potentially can be used in other attacks later that does.

Drone example: This method can allow the analyst to know certain semantics of the drone's flying patterns. A drone used for surveillance could easily be avoided if it is known where and when it will be.

4.2.3 Attack vectors

Attacks can affect different types of a system. An attack is often focused on a specific part, such as a specific sensor or the communication parts. Attacking a sensor is very dependent on the sensor itself and its type [20], while the communication focused attacks can be more widespread.

Message replaying

If it can be observed the a system responds in a certain way to certain behaviour it may be possible to recreate the action and then the same reaction, essentially performing a replay attack. Applying this on sensors could include showing certain images to a camera navigated drone, crafting specific radio- or light waves for drones using this information in its avionics parts.

Information theft

If an attacker uses eavesdropping on data being transmitted he could steal potentially value information. If the drone is used to collect sensitive or valuable data it could end in the hands of an undesired person. It could be data that is valuable for one company that is stolen by another, competitive company - either sensor data or videos and images.

Radio jamming

In this kind of deletion attack the wireless signal is "blocked" by sending out radio signals at the same frequency as the target make use of. This cause interference which effectively eliminates the original signal send from or to the target making communication impossible. Usually jamming is done over a wide spectrum of frequencies since it can be difficult to identify a single frequency amongst many. Of course jamming also affect everything else using a wireless signal in the spectrum unless the attacker uses a tube of some kind to make a directional jamming attack.

Message injection

When doing this kind of attack a message, which can be of any kind, is send out continuously. This is done either to saturate the network, like in a radio jamming attack, or to send information for corrupting messages.

Message alteration

The attacker receives a message which he modify and then sends off again. Depending on the goal of the attack the attacker can modify a couple of things: The sender information, receiver information or packet content. For some cases the attacker may change the information or he may delete parts of it.

4.2.3.1 WiFi specific attacks

WiFi is a protocol for wireless communication and a lot of WiFi specific attacks already exists with purpose of either gaining access to a device or an access point or to prevent others from accessing the access point thus eliminating the availability aspect of the CIA triad. Some of the known WiFi specific attacks could be relevant when looking for vulnerabilities and exploits in WiFi-based drones [21].

De-authentication

Broadcasting a de-authentication frame to both the WiFi access point and the client containing the MAC address of both stations will terminate the connection between them. If for example a mobile phone is used to control a drone with a WiFi connection, such an attack will make it impossible to maintain the connection and thus controlling the drone. This attack will compromise the availability of the drone. To perform this attack only a WiFi network card and the right software is needed. The software could be mdk3 or aircrack-ng both available for most Linux systems. After a successful de-authentication attack the stations can re-establish a connection and continue again. The attack is only valid as long as the de-authentication frames are broadcasted. A resilient hacker can continue the attack as long as he likes and the availability suffers as a result.

Shared Key Guessing

Often when you buy a wireless router the login credentials for the WiFi access point is set to vendor specific default value. The same scenario is possible with WiFi-based drones. If there even is a password associated with the WiFi hotspot it may very well be a default one which only requires an attacker to look up the specific vendor's manual. Other possibilities are trying some of the most passwords, such as 'root' or 'admin'. Even if the default password has been changed it may still be worth it to try some of the most common passwords used. There exists many lists of such and trying some of those might prove successful anyway. If an attacker gain access to the access point simply by guessing the password for the WiFi hotspot it is to be seen as a breach of authentication.

WEP Key Cracking

If the WiFi hotspot is password proctected with the WEP algorithm it may be easy for an attacker to crack the password as this standard uses very weak encryption. An attacker simply needs the right software and a WiFi network card in order to capture the packets sent from the base station. The WEP standard uses RC4, a stream cipher and an initialization vector of only 24 bit. As this is not enough bits to prevent re-use of keys the WEP standard is vulnerable to related-key attacks statistically after only around 10,000 packets. Attacking the key to gain access to a WiFi hotspot is an attack on the authentication. Most systems today have abondoned WEP for the newer and more secure WPA algorithm but some systems using WEP are still not uncommon. A weak encryption is not much better than no encryption at all.

WPA handshake sniffing

The WPA algortihm was developed as a more secure solution and is the replacement for WEP.

Often used in conjunction with the de-authentication attack in order to quicken the process of the access point and device performing a 4-way handshake that can be captured. After successfully capturing a WPA 4-way handshake it may be possible to crack the pre-shared key for the access point. If the access point uses a pre-shared key as authentication method, capturing the handshake might make it possible to crack the key with a dictionary attack. The WPA2 algorithm is the current and more secure standard that all devices today most support. It has support for TKIP and AES encryption, specifically the latter is considered very strong and is the recommended encryption algorithm by NIST[22, PR:7.1]. As the security of WPA2 is considered very strong, especially when using AES, a dictionary attack on the handshake may not be worth the time and resources.

Twin Access Point

Setting up an access point with the same SSID as one trusted by the user with the purpose of luring them in and connect to it can compromise the confidentiality. An attacker could use this to capture traffic sent and received by the user and anything not encrypted would be visible to the attacker. For a WiFi-based drone this could control signals, what do they look like, do they contain any necessary information to connect and control it such as a session- or unique ID and perhaps a pre-shared key. In any case it can lead an attacker to reverse engineer the control signal or even worse just see it in plain text.

Clear channel assessment

The way WiFi shares it's capacity is using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm. It works by having a preset interval called the Distributed Inter-Frame Space (DIFS) interval. When someone wants to send frames on the network channel the device will first wait the DIFS interval and if no other traffic has occurred then send the frame. If the channel is not clear it will chose a random value called the backoff interval. For every slot time it will listen for traffic on the channel. If the channel is clear the backoff interval will be reduced by one. If the channel is busy the backoff interval will freeze during that slot time. When the backoff interval are decreased all the way to zero it will send the frame is the channel must be empty in order to reach zero. An attacker could however attack the algorithm and keep sending frames on the channel to make it appear busy. That way the backoff interval will not decrease to zero and the frames will not be sent. This attack is compromising the availability of the network connection.

4.2.4 Network layers

When looking for exploits in a network it is important to know where an attack would be most likely to succeed. Looking at the network structure in Table 4.1 there are 7 different layers in the OSI model and 4 in the Internet Protocol Suite, also known as TCP/IP, to look at.

	OSI Model		**Internet Protocol Suite**
Host	7	Application	Application
	6	Presentation	
	5	Session	
	4	Transport	Transport
Media	3	Network	Internet
	2	Data Link	Link
	1	Physical	

Table 4.1: The OSI Reference Model and Internet Protocol Suite

Each layer has their own advantages and disadvantages but it all comes down to what type of attack is desired.

Implementing security measures in the different layers each have their advantages and disadvantages. As the OSI model is only a reference model while the Internet Protocol Suite (TCP/IP) is actually in use, the focus will be on this.

Looking at the security in each layer in the search for exploits these points are some interesting parameters to look at. If the security aspects are complex to implement or does not provide sufficient protection or if headers are exposed it may be possible to find a vulnerability to exploit.

Physical layer

Confidentiality	On link
Integrity	On link
Authentication	None
Replay Attack	No protection
Traffic Analysis	Protection on link

The physical layer is the most low-tier layer and the most simple. There is no authentication and thus no replay protection, but does secure the entire traffic on a single link. Even source and destination addresses are secured by this. The drawback is the security is only on the link and is therefore vulnerable in a switching node, where it might be possible to launch an attack.

Internet layer

Confidentiality	Between hosts and sites
Integrity	Between hosts and sites
Authentication	Hosts and sites
Replay Attack	Hosts and sites
Traffic Analysis	Host and site information exposed

The internet layer is the one responsible for exchanging IP packets over the network and where the IP resides. Security properties can only happen between hosts and sites. Might not be the best option to try application specific replay attacks but may reveal possibly useful patterns in a traffic analysis.

For drones, traffic analysis in this case might not be this relevant as the meta data of a packet is not as interesting as the payload.

Transport layer

Confidentiality	Between apps, hosts and sites
Integrity	Between apps, hosts and sites
Authentication	Both user, host and site
Replay Attack	Between apps, hosts and sites
Traffic Analysis	Protocol and host and site info exposed

The transport layer builds on top of the internet layer and handles the protocols used on top of the IP packets such as TCP or UDP.

Application layer

Confidentiality	Only between apps
Integrity	Only between apps
Authentication	User
Replay Attack	Only between apps
Traffic Analysis	Only payload is protected

The protection is probably easiest to implement in the application layer as it is on a per application basis. This however makes it vulnerable to replay attacks and traffic analysis while the apps is handling confidentiality, integrity and authentication separately.

On a drone there may not be different apps and may just be a system on a chip but attacking the application layer could be a good first step with passive attacks by eavesdropping and traffic analysis.

Even if the content is encrypted and therefore unreadable it might still be subject to a replay attack.

4.3 Risk Management Methods

When performing a risk management operation there exist a variety of different modelling methods and tools each having focus on their own niche. Choosing between these methods is a choice of which viewing angle is preferred. Some of the methods are standardised and more used than others.

- AGRA
- CORAS
- DREAD
- ISO 27000
- ISO 31000
- ISRAM
- OCTAVE
- OWASP
- STRIDE

In this thesis the selected methods are ISO 27000, more specifically the subsection ISO 27005 because it's an international standard and describes information security risk management.

The CORAS method will also be used because of its tools to create diagrams to create a visual impression of the stakeholders, risk and consequences associated with the risk management.

4.3.1 ISO 27005 - Information Security Risk Management

The ISO 27005 is drafted by the International Organisation for Standardisation to give guidelines for organizations, mainly businesses, in Information security risk management.

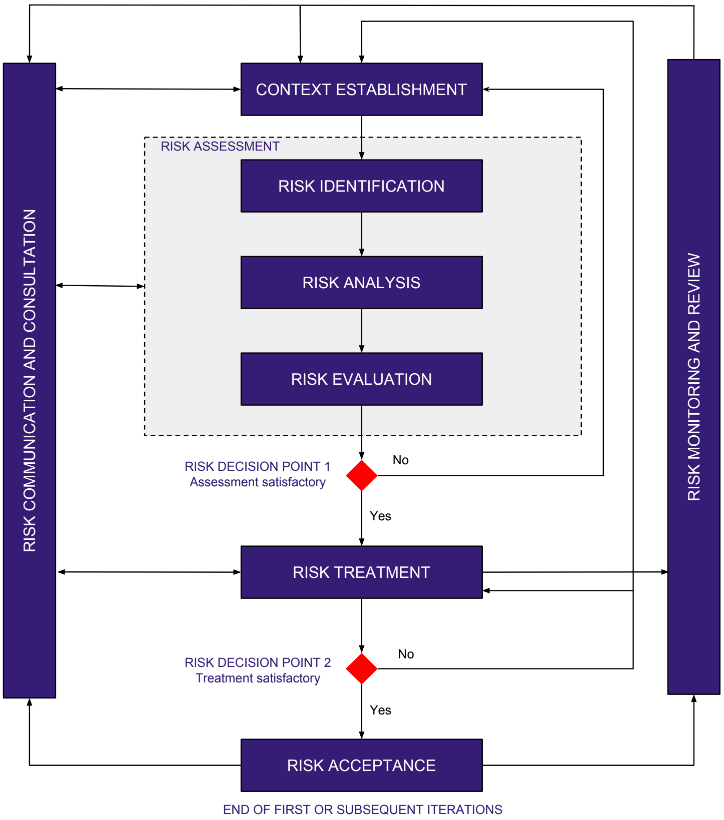


Figure 4.7: Risk management chart recreated after the one in ISO 27005

Figure 4.7 show an information security risk management process which can be used both in risk assessment and risk treatment. The process can, and should, be conducted iteratively in order to get as much information out of the process as possible. The iterative process may also lead to new information about findings in previous iterations.

The management process consists of the 8 phases:

1. Context Establishment
2. Risk Identification
3. Risk Analysis
4. Risk Evaluation
5. Risk Treatment
6. Risk Acceptance
7. Risk Monitoring and Review
8. Risk Communication and Consultation

where the phases from 2 through 6 concerns the actual risk management.

4.3.1.1 Context establishment

In this phases the all the relevant information regarding the organisation is gathered in order to do the risk management. The purpose of the information security risk management should be defined, setting up the scope and boundaries, as well as creating a suitable organization to operate the process.

Apart from the information gathering the Context establishment phase also include setting up basic criteria for the risk management process:

Risk management approach

A risk management approach should be selected or developed such that a set of basic criteria regarding evaluation, impact and acceptance of risks can be set up. The approach chosen should be depending on the scope and objectives identified.

Risk evaluation criteria

In order to evaluate the information security risk of the organization a risk evaluation criteria should be developed. To do this some considerations needs to be made including: critically of information assets, legal and regulatory requirements, and stakeholder expectations and perceptions.

Impact criteria

The impact criteria should be specified with respect to how severely the organization is affected in terms of damage and/or cost in case of a information security incident taking place. During this process several considerations should be made including classification levels, loss of value and damage of reputation.

Risk acceptance criteria

The organization should develop and specify its risk acceptance criteria considering the policies, goals, objectives and interests of stakeholders of the organization. Whether a risk should be accepted or not is depending on business criteria, legal and regulatory aspects, operations, technology, finance, and social- and humanitarian factors.

4.3.1.2 Risk Identification

As the first part of the Risk Assessment the purpose of risk identification is to get an understanding of the risks as to what causes them, how it is possible and what they affect.

In order to identify the risks the organization should identify:

- Assets
- Threats
- Existing controls
- Vulnerabilities
- Consequences

which, when viewed as a whole, makes up the risks.

In a drone environment however the assets are depending on who or what is considered. If the focus is on the pilot he will most likely be interested in the security and safety of the drone, but this is not true for the bystanders who prioritises safety for humans and property, and privacy above all else. This deviation in how assets should be interpreted in a drone environment compared to the norm in asset identification affects the rest of the risk identification.

Identification of assets

An asset is anything which have a value for the organisation [23] and for that reason they are (to some extend) worth protecting against inner and outer threats.

The assets of an organisation are are divided between eight groups:

- Hardware
- Software
- Data
- People
- Documentation
- Supplies
- Intellectual
- Reputation

For each asset and owner should be identified, who may give information as to the value of the asset for the organization. The reason that a owner should be identified is to provide responsibility and accountability for the assets.

In a drone environment however the groups listed above are not enough to describe the assets as the *privacy* and *safety* need to be considered as well. They can be seen as external assets from the drones perspective but are just as important since they are of value to individuals in the environment. For this reason they should also be included when talking about assets in relation to drones.

Identification of threats

A threat is an action leading to unwanted incidents which may harm one or more assets. The source of the threat should also be identified in addition to a likelihood estimation. The threat can either be of human or non-human origin and in case it is human then the threat could be accidental or deliberate. The likelihood estimation should be made in cooperation with the identified asset owners in order to give fitting estimate the occurrence of each threat.

Identification of existing controls

The controls which may be already implemented should be identified and checked to make sure that they work as intended. The reason for doing this is to prevent unnecessary work later on if the existing control mechanisms are found to be functioning acceptably. If however a control is found to be insufficient, inefficient or unjustified then considerations should be made whether the control should be removed, replaced or stay because removing or replacing it would cost more than what is gained.

If there are any controls that are planned to be implemented then they should be treated as the already implemented control.

Identification of vulnerabilities

The vulnerabilities of an organization are not by themselves harmful but they can be exploited by threats in order to harm the organizations assets. How the vulnerabilities have emerged are depending on where in the organization they are located such as:

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

If there does not exist a threat that are found to exploit a certain vulnerability then a control mechanism may not be needed but monitoring of the vulnerability should be established. This of course is a list of the known possible threats. Unknown threats are not possible to identify, as they are unknown, but they might still exist. The goal is to create the most thorough vulnerability identification as possible to later eliminate most threats even some of the unknown unknowns.

Identification of consequences

The consequences that losses confidentiality, integrity or availability of assets due to a threat exploiting one or more vulnerabilities in the organization should be identified. The effect of a consequence on an assets may be temporary or of a more permanent nature depending on the asset itself and the threat.

The organization should also identify the operational consequences involved, including:

- Investigation and repair time
- Work time lost
- Opportunity lost
- Health and Safety
- Financial cost of specific skills to repair the damage
- Image reputation and goodwill

When identifying the impact of the consequences the impact criteria created in the Context Establishment should be taken into consideration.

4.3.1.3 Risk Analysis

The first step of the risk analysis is to determine how the analysis should be performed. When the organization has found a suitable analysis the consequences and incident likelihood for each risk are assessed. The final step of risk analysis is to make a level-of-risk determination.

Risk analysis methodologies

A risk analysis methodology can be qualitative, quantitative or combination of them. Both of the analysis uses scales in the form of a risk matrix in order to rank the risks giving an idea of which of them would harm the organization the most either by the consequences, incident likelihood or both.

Qualitative In a qualitative analysis the scale is made from qualifying attributes, for instance [Low, Medium, High], assigned to the impact and likelihood. The values are based on the expected impact and likelihood for each risk through communication with the asset owners. Due to the kind of ranking a qualitative analysis can be used as a initial screening to identify risk which require further or a more detailed analysis.

Quantitative In a quantitative analysis the scale is made from numerical values assigned to the impact and likelihood. The values are based on previous documented incidents either registered by the organization or third parties. Because of this this kind of analysis is not suited to handle new threats. For known risks which may already have been documented by the organization a quantitative analysis has an advantage since these risks may have been analysed previously.

Assessment of consequences

The assets identified are valuated according to how important they are for the organization to reach the goals set by the organization. In case an asset is found to be very valuable then the impact on the organization in case an unwanted incident occurs which affect the asset will be great. The criteria on which the impact is measured may be based on the loss of money, reputation or that which the company counts as a key factor to their business processes.

From the valuation the incidents that may harm one or more assets can then be ranked according to the affected asset having the highest value to the organization. Thus an incident affecting both low and high valued assets will be ranked in accordance with the high valued assets.

Assessment of incident likelihood

The likelihood of an incident occurring is determined by identifying how often a threat may occur and how easy it is to exploit a vulnerability. This can be done from experience or by consulting third parties who may have some kind of statistical data concerning the occurrence of certain threats.

Level of risk determination

From the assessment of the consequences and incident likelihood the estimated level of risk is determined for each threat. This is a combination of the two values depending on whether the risk methodology chosen was qualitative or quantitative. If the quantitative methodology was chosen then the result will be numeric value derived from the consequence and likelihood values whereas if the qualitative methodology was chosen then values derived from both consequences and likelihood can be kept intact.

4.3.1.4 Risk Evaluation

In this phase the estimations determined for each threats, as a result of the Risk Analysis, are evaluated in accordance with the risk evaluation criteria and the risk acceptance criteria defined in the Context Establishment. The evaluation can advantageously be carried out by using a risk matrix in which all the risk a placed according to the ranking from the Risk Analysis. The risk evaluation criteria and the risk acceptance criteria should be integrated in the risk matrix to give an overview of which risks are acceptable and which are not.

The Risk Evaluation is used for decision-making on future activities in the treatment of the risk which are found to be on a not acceptable level. In following iterations of Risk Management the results from the Risk Evaluation may be used as a basis for comparison for the Risk Assessment to identify risk which may have changed since the last Risk Management process was conducted.

4.3.1.5 Risk Treatment

In the Risk Treatment phase control are introduced in order to bring the level of risk of down to an acceptable level in accordance with the risk acceptance criteria. Controls should only be implemented for risk which do not meet the risk acceptance criteria to prevent use of unnecessary resources.

When implementing a control mechanism the following should be taken into consideration:

- The result from the Risk Assessment
- The cost of implementing the control
- The advantage of implementing the control

The controls can be of four different types being: Modification, Retention, Avoidance and Sharing.

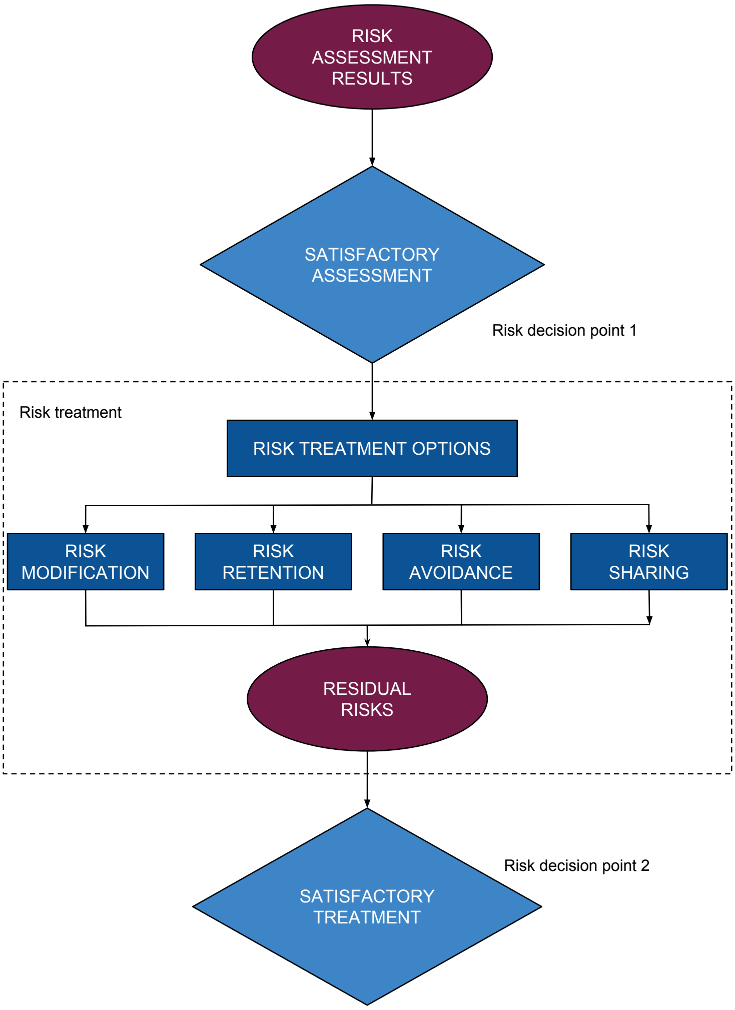


Figure 4.8: Risk treatment chart recreated after the one in ISO 27005

Risk Modification

The purpose of the risk modification is to introduce controls meeting the requirements which were identified during the risk assessment and risk treatment.

This is done in order to get an acceptable risk level during the reassessment procedure with respect to the risk acceptance criteria.

The modification of a risk can include one or more of the following:

- Correction
- Elimination
- Prevention
- Impact minimization
- Deterrence
- Detection
- Recovery
- Monitoring
- Awareness

Which of them to choose depend on several constraints which must be consulted before implementing the risk modification procedure:

- Time
- Financial
- Technical
- Operational
- Cultural
- Ethical
- Environmental
- Legal
- Ease of use
- Personnel

The constraints may not always be the same modifications since the internal procedures and the environment the organization is operating in also have an effect on which of the constraints will be present.

Risk Retention

In case a risk for some activity does not exceed the level of risk acceptance then there is no need for implementing risk treatments to handle the risk. This decision should be made on the basis of where in the risk evaluation matrix the risk is located.

Risk Avoidance

The decision to avoid a risk by stopping an exiting or planned activity may be the best action to make if the cost of implementing risk treatments are to high or the benefits of doing so are minimal. The avoidance of a risk often means that the activity is changed such that the risk is not existing, minimal or under some kind of control.

Risk Sharing

If the competences for managing a risk are not present then sharing the risk with an external third party is an option in order to handle the risk. However doing so new risks may arise or existing risks are modified which could require additional risk treatment.

Residual Risk

When the plan for the control implementations have been made the residual risks should be determined. This a part of the output from the Risk assessment process along with a risk treatment plan. The residual risk consists of the expected level of risk following the implementation of the risk treatment.

4.3.1.6 Risk Acceptance

In the Risk Acceptance phase the acceptance of the risks and the person responsible for making the decision are registered such that in the event of an unwanted incident the treatment can be inspected and the responsible can be held accountable.

For a risk to be accepted it must primarily fulfill the risk acceptance criteria made in the Context Establishment but it is possible to accept it if for instance the cost of lowering the level of risk is to high in relation to the benefits. In such cases it is important to document why the risk is accepted for use in future Risk Management processes and in case of an unwanted incident.

4.3.2 CORAS

CORAS is a UML based risk assessment model originally developed as an EU-funded project between 2001 and 2003 but have seen further development after being open-sourced.

CORAS is consist of three parts:

1. The CORAS Language
2. The CORAS Tool
3. The CORAS Method

4.3.2.1 The CORAS Language

The CORAS language consists of symbols and connections, where some of the connections are shown in Fig. 4.9.

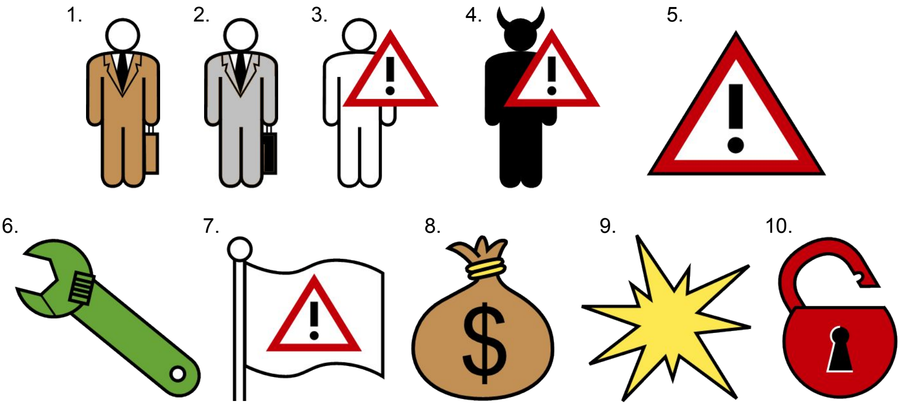


Figure 4.9: The symbols in CORAS: **1.** Stakeholder, **2.** Stakeholder (grey), **3.** HTA, **4.** HTD, **5.** Risk, **6.** Treatment, **7.** NHT, **8.** Asset, **9.** Unwanted Incident, **10.** Vulnerability

CORAS distinguish between two kinds of assets: Direct and Indirect. An indirect asset is an assets which can only be harmed through other assets [24]. In addition the source of threats is divided between three kinds: Human Threat Accidental (HTA), Human Threat Deliberate (HTD) and Non-Human Threat (NHT).

The symbols are used to create five kinds of diagrams:

Asset diagram Contain the direct and indirect assets as well as the party which the analysis is made on behalf of. How the assets affect each other in case of a unwanted incident is shown with arrows.

Threat diagram Contain the sources, vulnerabilities and unwanted incidents related to the threats, as well as the assets affected.

Risk diagram Used to give the customer an overview of the results in the Threat diagrams and can also be used to show the affected Indirect assets.

Treatment diagram A kind of Threat diagram that contains the proposed treatments going to be implemented as controls to modify the risks.

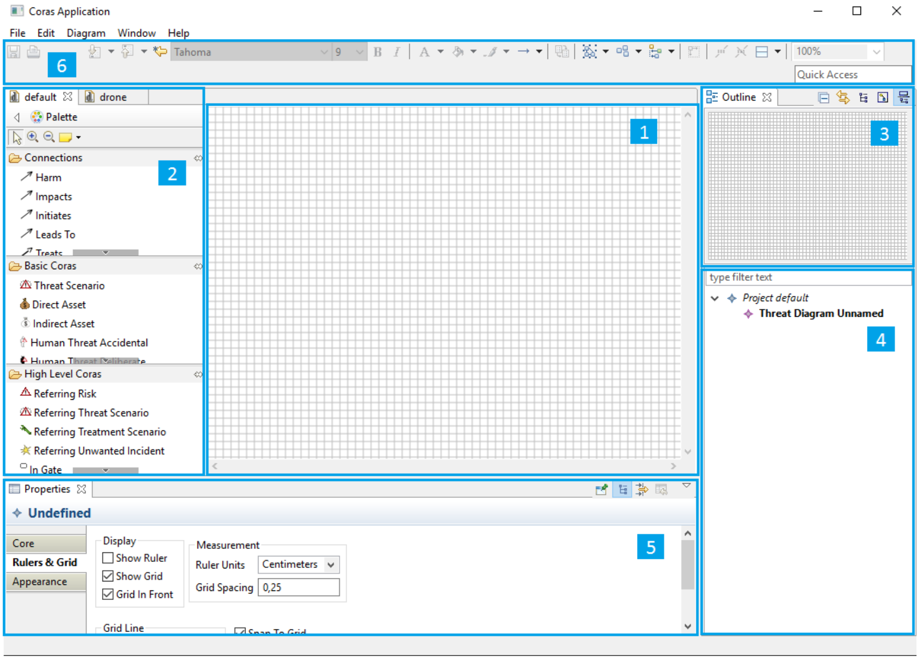
Treatment Overview diagram A combination of the Risk diagram and Treatment diagram which is used to give the customer an overview of the risks and the treatments.

4.3.2.2 The CORAS Tool

In order to create the diagrams the CORAS tool is needed. It is written in the JAVA language

The tool, shown on Fig. 4.10, is build up by 6 elements:

1. A canvas, where the CORAS diagrams are created, placed in the middle of the window.
2. A symbol and connection palette located in the left side of the window.
3. A mini clipboard giving an overview of the entire clipboard. It is located in the upper right corner of the window.
4. A project list showing the currently open projects and the diagrams in them. It is located in the lower right of the window.
5. A properties view showing information about the diagram, symbol and connection currently selected. It is located in the bottom of the window.
6. A toolbar containing editing options for the diagrams, symbols and connection. It is located in the top of the window.



□ Show Ruler
☑ Show Grid
☑ Grid In Front

Ruler Units: Centimeters
Grid Spacing: 0,25

Figure 4.10: Screenshot of the CORAS tool

The tool is primarily meant to be used in brainstorming sessions to give a visualized understanding of the risk assessment, but also as a way to present the results to the customer.

The tool is available for free on the CORAS website `http://coras.sourceforge.net`.

4.3.2.3 The CORAS Method

The CORAS method consists of 8 steps

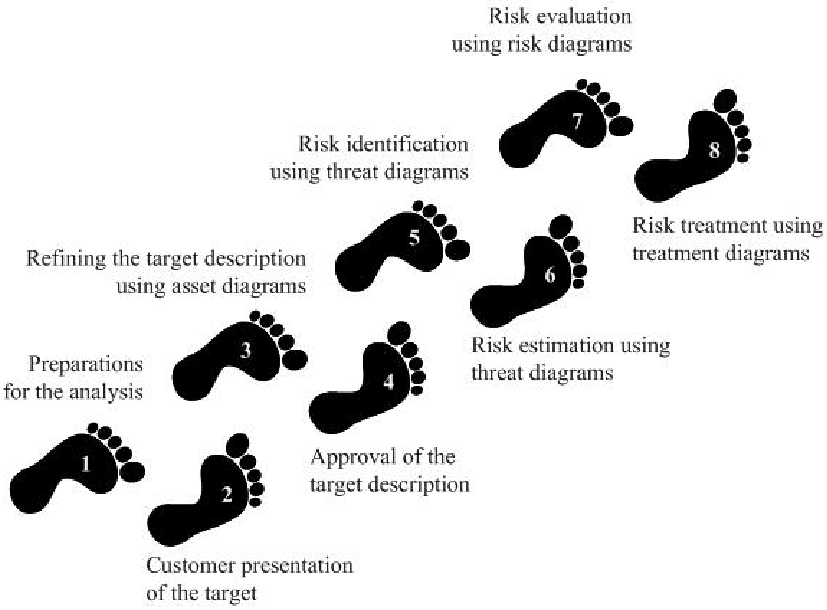


Figure 4.11: The eight steps of the CORAS Method [24]

Step 1 In the first step considerations are made such as making a roughly defined scope and focus of the analysis. Preparations for the actual risk analysis is also made so that the analysis team is ready to start their work.

Step 2 In the second step an information meeting is set up with the customer who should put forward such as their goals and targets of the analysis. Agreements are also made between the analysis team and the customer as to what should be protected, a joint terminology and which assumption there is to be made.

Step 3 In the third step a more thoroughly understanding of the target and customer goal is reached. To do this a second meeting might be set up in which the analysis team should make a presentation for the customer. This presentation should include:

1. Target presentation as understood by the analysis team
2. Asset identification
3. High-level risk analysis

On the basis of the presentation the customer is able to give feedback to help the analysis team to refine the understanding of the target, assets and goal of the risk analysis.

In this step one or more Asset diagrams are created.

Step 4 In the fourth step the target and goals of the analysis is agreed upon between the analysis team and the customer. This could involve creating a risk analysis description which include all the information gathered by the analysis team in the previous steps. In addition the analysis team should create scales for likelihood and consequences as well as risk evaluation criteria. The description should then be approved by the customer in order for the analysis team to move forward to the next steps.

Step 5 In the fifth step people with different competencies are gathered to participate in a workshop with the goal to identify unwanted incidents, threats, vulnerabilities and threat scenarios. In the workshop a technique called structured brainstorming is used which, in connection with the multi-competencies group, increases the number of risks identified.

In this step one or more Threat diagrams are created.

Step 6 In the sixth step the likelihood and consequences for the unwanted incidents, threats, vulnerabilities and threat scenarios identified in Step 5 are estimated. The process can be conducted as a in Step 5 with a structured brainstorming where each participant make a likelihood and consequence estimation which is to be discussed with the rest of the group. The collective result of the likelihood and consequence estimation is used to make decisions as to whether a risk is acceptable or some treatment is needed to handle it.

In this step the Threat diagram created in Step 5 is used.

Step 7 In the seventh step the results from Step 5 and 6 are presented to the customer to give them a overall picture of the risk analysis. The goal is to determine the risks which are to be considered necessary to introduce treatments against. The presentation to the customer may give some extra inputs and/or adjustments of the analysis so far. An additional goal of this step is also to estimate and evaluate the risks which may harm indirect assets.

In this step one or more Risk diagrams are created.

Step 8 In the eighth step treatments are found in order to reduce the likelihood and/or consequences of the identified risks from Step 7. Each of the treatments are addressed with respect to the cost of introducing them prior to the final treatment plan construction.

In this step one or more Treatment diagrams are created by using the Risk diagrams from Step 6. When presenting the risks and proposed treatments to the customer a Treatment Overview diagram could be made.

4.4 Countermeasures

It is important to realize that it never possible to make a system secure. The only factor which prevent access to the system, is time. By applying more resources the time needed to penetrate the defences can be reduced. If the time needed is too long it will deter more attackers from attempting to gain access to the system. In order to counter penetrations one can introduce one or more measures to increase the difficulty of gaining access if you are not authorised. There are several ways to so, whether it may be added layers of complexity that takes time to circumvent or strong authentication where brute forcing will not be possible in a lifetime.

4.4.1 Cryptography

A method used to make data unreadable by applying one or more algorithms. These algorithms often makes use of mathematical problems such as the discreet logarithm problem or the factoring problem. The reason for using these problem is that they are easy to compute one way but hard to compute the other way.

In cryptography the use of one or two keys is required to do the decryption in order for the authorized person to get access to the system or some data. The number of keys needed is determined by whether the algorithm used is symmetric or asymmetric. If the encryption is symmetric then only one key is used whereas two key are used for asymmetric encryption.

By using a cryptographic algorithm the system needs to use energy, computational power and memory. If the system is already lacking these resources then problems such as power shortage, CPU- and memory overload most likely will arise. To avoid these problems the concept of lightweight cryptography can be used to lower the resource requirements at the cost of the cryptographic strength.

When doing lightweight cryptography one must choose only one of the following resources to to focus on:

- Power
- CPU
- RAM

The usage change of one of the resources will inevitably also have an impact on the other two resources, but it can be either positive or negative. The reason for this is that sometimes it is possible to somewhat improve the usage of one other of the resources. Which of the three resources to choose is depending on the system and the the resources available. It is clear that in system with plenty of power and memory the best choice would be to optimize the CPU usage.

4.5 Hardware and software

In the process of discovering vulnerabilities in a system communicating wirelessly some properties are needed to be known. Firstly, the frequency the communication is using is needed. For example, WiFi often use 2.4 GHz while GSM often use 900 MHz or 1800 MHz. This is needed in order to use an antenna capable of transmitting and receiving the desired frequency. Once an antenna is acquired it is possible to use an application such as Wireshark to scan the frequency in order to perform a traffic analysis.

Chapter 5

Risk Assessment

The results of this chapter will be the first part of the model developed to manage the risks that may occur when flying with drones. The second part being Risk treatment will be examined later on in .

To analyse the risks, which may rise when handling drones, mainly the ISO 27005 approach will be used whereas CORAS only is used in an auxiliary manner to give a visual understanding of the different parts of the analysis and how they are related. However some of the terminology used in CORAS will also be used in the analysis to make a more clear connection between the two models.

None of the models however have the support for multiple stakeholders because they are created for a commercial context. Since the environment for a drone is not of such a kind, some changes needs to be made in the analysis to be able to include the identified elements in a drone environment.

For this reason most of the Risk Assessment is divided into three part each of them focusing on one of the stakeholders shown in Fig. 4.1: the drone, the pilot and the bystanders. For good measure, the three stakeholders defined as follows:

Drone The system which makes up a fully functional UAV

Pilot The person flying the drone whether it is the owner or not.

Bystander Any person within the flight radius of the drone.

The Context establishment can be applied for each of the stakeholders and therefore it is only made once.

5.1 Context Establishment

The analysis methodology that is going to be used is a qualitative and is therefore a survey of the security risks involving drones in general. The scales for the consequences and incident likelihood are divided into five levels:

- Very Low
  - The consequences are not notable
  - An incident may occur years apart
- Low
  - The consequences are mentionable
  - An incident may occur within months or a few years
- Medium
  - The consequences are significant
  - An incident may occur months apart
- High
  - The consequences are severe
  - An incident may occur within weeks or a few months

- Very High
  - The consequences are devastating
  - An incident may occur within days or weeks

The following color-coded table will be used to classify the risks identified in the analysis:

		Incident likelihood				
		Very Low	Low	Medium	High	Very High
Consequences	Very Low	🟩	🟩	🟩	🟨	🟨
	Low	🟩	🟩	🟨	🟨	🟨
	Medium	🟩	🟨	🟨	🟨	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Very High	🟨	🟨	🟥	🟥	🟥

Table 5.1: Risk Matrix

The green colored indices are considered to be low priority risk-level. Risks that are placed here should not be handled unless the cost and time involved are minimal. The yellow colored indices are considered to be medium priority risk-level. Each risk placed here should be seen as potential candidates for control modification. The red colored indices are considered to be high priority risk-level. For any risk placed here controls should be introduced unless the cost and time are to great in relation to the benefits.

5.2 Risk Identification

In this section the risk identification will be divided into three parts each focusing on either the drone, the pilot or the bystanders as the stakeholder. This include identifying assets, threats, controls, vulnerabilities and consequences for each stakeholder.

In the end of the section CORAS will be used to visualize the findings of the three risk identification parts.

5.2.1 The Drone as a stakeholder

Even though the drone is not a alive it should be seen as a stakeholder as it has dependencies in order to function properly.

Identification of assets

To identify the assets for a drone, Fig. 3.1:

Hardware	Battery, Power supply, IMU, Sensor array, Radios, Transceiver, Telemetry module, Flight controller, On-board data storage, ESCs, Motors and Propellers
Software	Internal Algorithms
Data	Control signal, Telemetry data and Sensor data

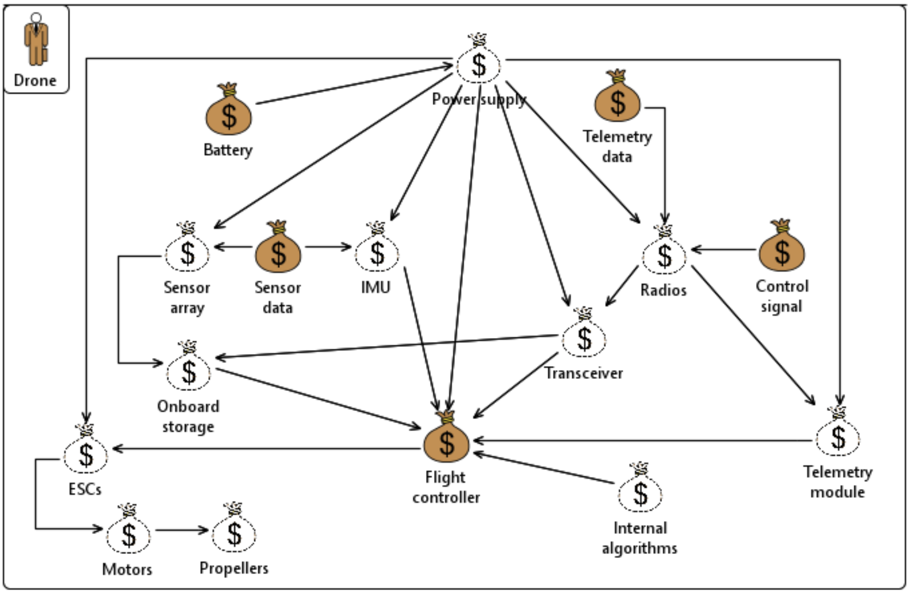


Figure 5.1: Asset diagram of a drone

Identification of threats

Battery depleted

A sudden loss of power can be catastrophic for the drone as an impact after a fall to the ground can damage the components of it. A power loss also makes the drone inoperable.

The unwanted incident originating from power loss are:

- Unusuable battery
- Drone crash

Invalid input

The drone getting invalid input - either from the control signal, telemetry module or from the sensor array - can make the drone behave in unexpected ways. The invalid input can arise in different forms; malformed data, too much data during a time frame, corrupt data, unexpected data when awaiting other data or not receiving data when it is expected. In another scenario the drone could get invalid data without knowing before its to late to rectify the mistake specifically thinking of the drone crashing and damaging hardware.

The unwanted incident originating from invalid input are:

- Internal system crash
- Drone crash

Identification of controls

Some controls have been identified:

Battery monitor Can be used in further controls

Return to starting point when low on battery The starting position which is stored in the drone is used along with the GPS to get back to the pilot.

Identification of vulnerabilities

Some vulnerabilities have been identified:

Poor quality battery Most batteries cannot support extended flight which may be due to the battery being of a poor quality.

No energy optimization Most batteries cannot support extended flight which may be due to the energy usage not being optimized.

No input validation The data received from both the control signal and the telemetry link is often not validated before used or stored.

Identification of consequences

The consequence originating from both the identified threats is that the drone crashes. In the crash some individual parts of the drone may be damaged such as the propellers, radios or other of the identified hardware assets.

5.2.2 The Pilot as a stakeholder

In the drone environment the stakeholder who has the most to lose is the pilot. The main reason for this is because of the relation between the pilot and the drone which is of a very special kind. The pilot is, in some cases, the owner of the drone and this makes the drone an asset to the pilot. Since the pilot is controlling the drone the control signal and the telemetry data, which could be stored on an onboard storage device, are assets as well as the packages which may be carried by the drone. The pilot also have assets connected to safety specially the drone, himself and also bystanders. This is because not just the drone environment is important in this matter as the world beyond the environment should also be taken into account. To be considered are the reputation of drones in general and the pilot, and also the legal liability of the pilot.

Below the identified assets are summarised:

Hardware	Drone and Packages
Data	Telemetry data (streamed video, GPS, etc.), Control signal and Stored data
Reputation	Legal liability of pilot, Reputation of drones and Reputation of pilot
Safety	Human safety and Drone safety

The connection between the identified assets for the pilot is shown in Fig. 5.2.

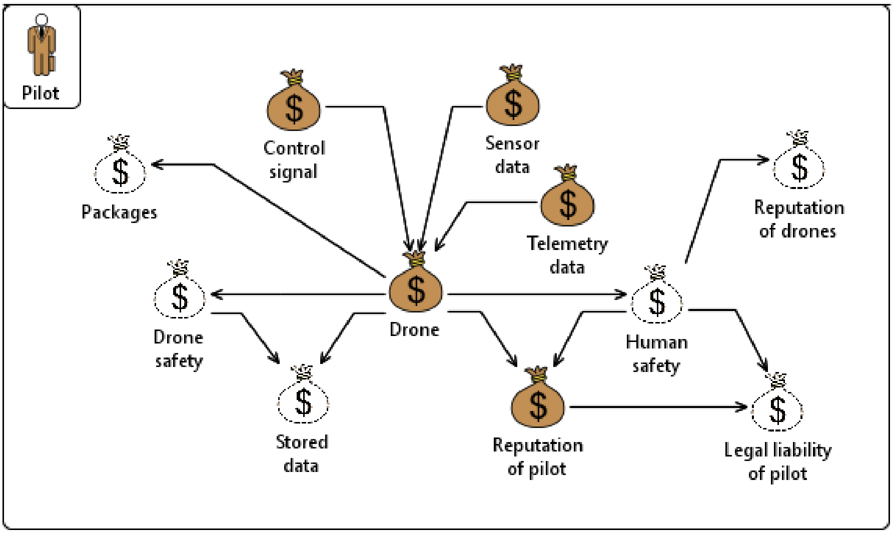


Figure 5.2: Asset diagram for the pilot and how the assets affect each other

On the figure it is seen that the drone is affected by the control signal and telemetry data. The drone then affect the rest of the assets either directly or through other assets. One should specially notice that Human safety affect the legal liability and reputation of the pilot as well as the reputation of drones. This makes Human safety the most import indirect asset. Furthermore by harming the Reputation of the pilot the Legal liability of the pilot may also be harmed in case someone choose to report the incident to the authorities.

Identification of threats

A number of threats and unwanted incidents have been identified:

Pilot has insufficient competencies

For a pilot to fly a drone he needs the competencies for flying them such that anybody or anything gets damaged. When ordinary people buy a drone they usually do not have the skills to fly them in a proper manner and it may take some time to get these skills. In addition some technical knowledge may also be required to for instance calibrate the drone or set up the telemetry link.

The unwanted incident originating from insufficient competencies are:

- Drone crashes
- Flying in populated area

Poor password management

If the drone has some for of encrypted communication then the pilot should know about proper password management. For ordinary people this is not always the case which could cause some trouble for drones having a password protected connection specially because the standard password used often can be found on the Internet. Having a poor password management does not directly cause unwanted incident but it can be an important factor in both active and passive attack.

Drone looses power

Most drones for sales in shops do not have a flying time above 10 minutes which can cause it to crash in case the pilot keep in mind that it needs to be recharged.

The unwanted incident originating from the drone losing power are:

- Drone crashes

System crash during flight

Many drones on the market are cheaply made so the hardware and software in the drone are not of the best quality. The internal system of the drone can because of this have undiscovered defects which can lead to a system crash.

The unwanted incident originating from a drone system crash are:

- Drone crashes

Drone link problems

The data link between the pilot and the drone can be of a poor quality do to low construction budgets. This can potentially cause the data transferred from the drone to the pilot and the other way around to be corrupted.

The unwanted incident originating from problems in transferring data are:

- Compromise of availability of control signal
- Compromise of availability of telemetry data

Eavesdropping

A passive attack performed to get data from the control signal or telemetry link. Even though the attack is not particularly harmful by itself it can be used in further attacks of a more malicious nature.

The unwanted incident originating from eavesdropping are:

- Compromise of confidentiality of control signal
- Compromise of confidentiality of telemetry data

Traffic Analysis

An attacker can get meta-data from analysis the traffic between the pilot and the drone. This may lead to information gathering on the links themselves which can be used in malicious attacks. Performing traffic analysis does not directly lead to unwanted incidents.

Fabrication Attack

Performing a fabrication requires that the attacker have extended knowledge about how the pilot and the drone communicate which can be achieved by having performed Eavesdropping and Traffic analysis attacks. The attack violates the integrity of the control signal and/or telemetry data, and can possibly lead to a hostile takeover of the drone.

The unwanted incident originating from a fabrication attack are:

- Compromise of integrity of control signal
- Compromise of integrity of telemetry data

Modification Attack

As with the Fabrication attack the Modification attack requires some knowledge about the communication between the pilot and the drone but not necessarily as extensive. This is because the modified data is not required to make sense to the receiver. In the worst cases the attacker is able to take control of the drone.

The unwanted incident originating from a modification attack are:

- Compromise of integrity of control signal
- Compromise of integrity of telemetry data

Deletion Attack

Making sure that the pilot and the drone are unable to communicate either by the control signal and/or the telemetry link are an effective way of sabotaging the control over the drone. To do it effectively a Traffic analysis attack may be required to identify the frequency used in the communication.

The unwanted incident originating from a deletion attack are:

- Compromise of availability of control signal
- Compromise of availability of telemetry data

The direct assets and the unwanted incidents are now linked in the list below:

- **Drone**

  D1 Crash of drone
- **Control signal**

- *C1* Compromise of confidentiality of control signal
- *C2* Compromise of integrity of control signal
- *C3* Compromise of availability of control signal

- **Telemetry data**
  - *T1* Compromise of confidentiality of telemetry data
  - *T2* Compromise of integrity of telemetry data
  - *T3* Compromise of availability of telemetry data
- **Reputation of pilot**
  - *R1* Flying in populated area

The table below summarise the threats, unwanted incidents and their source for each direct asset:

Unwanted Incident	Threat	Source
Drone		
D1	Drone looses power	No power on battery
D1	Insufficient competencies	Pilot
Control Signal		
C1	Eavesdropping	Passive attacker
C2	Fabrication attack	Active attacker
C2	Modification attack	Active attacker
C3	Deletion attack	Active attacker
C3	Drone link problems	Poor quality tech.
Telemetry Data		
T1	Eavesdropping	Passive attacker
T2	Fabrication attack	Active attacker
T2	Modification attack	Active attacker
T3	Deletion attack	Active attacker
T3	Drone link problems	Poor quality tech.
Reputation of pilot		
P1	Flying in populated area	Pilot

Table 5.2: The unwanted incidents, threats and source which can affect the Direct Assets.

Identification of controls

Some controls already exist in order to modify the threats against the identified assets.

Frequency hopping Hopping between frequencies within a spectrum can prevent loss of connection to the controller.

Unique controller ID Having a unique ID for the controller the drone can check if the received data is genuine.

Handshaking protocol Using a handshake protocol when the drone is turned on can be used to check if the received data is genuine.

Return to starting point This can happen in two cases:

- when the drone is low on battery power
- when the signal from the controller is lost

Identification of vulnerabilities

Vulnerabilities which can be exploited by the identified threats are found to be:

Poor quality technology Drones build with a low budget often also apply the poor quality parts.

Standard password on control signal and telemetry data Instead of making a unique password for each manufactured drone companies tend to use the same password for all drones.

Unstable connection Can occur as a side effect of the drone being created on a low budget.

The pilot has limited technological knowledge True in some cases the buyer of the drone do not have the technological skills to for instance calibrate the drone.

The pilot has insufficient competencies To fly a drone it takes a lot of experience but this is almost never the case.

Insufficient connection protection Drones do often not have a protected communication link to the controller.

Identification of consequences

If case the drone crashes then it may be damaged to such an extend that it is broken making it unusable. Another possibility is that the drone is not broken but is stolen after the crash landing removing it from the possession of rightful owner. In case the pilot do not have the required competences to fly a drone he may cause the drone to crash or fly over a populated area unintentionally. If the pilot is identifiable in these cases his reputation will most certainly be harmed and may lead to legal consequences ranging from a ban on flying drones to fines and imprisonment.

By attacking the drone with a fabrication or modification attack the Active attacker may be able to use the drone with malicious intent such as filming bystanders. In case the attacker is not a experienced drone pilot the drone may crash possibly harming humans or property. If the attack can not be proved to have happened then the owner of the drone may be harmed in a legal sense.

5.2.3 The Bystanders as stakeholders

To look at the bystanders as stakeholders is a little special as they have nothing directly to do with the drone, but are a part of the drone environment. As such they do focus only on the privacy and safety of themselves and their property.

The assets of the bystanders are identified to be:

Privacy	Human privacy, Behavioral patterns
Safety	Human safety and Property safety

Only the Behavioral patterns are depending on another asset namely the Video recording covering both video and pictures.

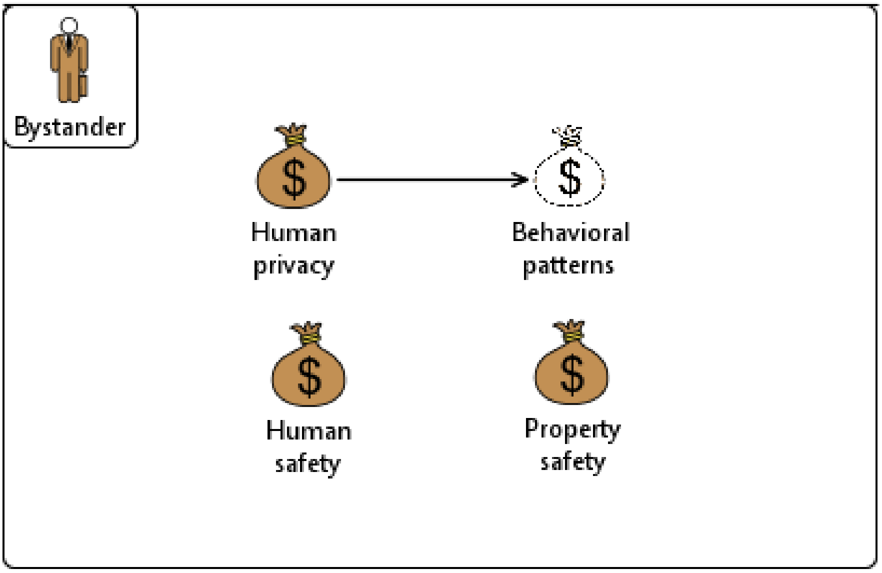


Figure 5.3: Asset diagram for bystanders

Identification of threats

The following threat and connected unwanted incidents have been identified for the identified assets:

Pilot has insufficient competencies

The pilot in this sense can be either the owner or an attacker who has gained control over the drone. If either of them have the required competencies to fly the drone in a safe manner then the bystander or property can be harmed.

The unwanted incident originating from insufficient competencies are:

- Human injury
- Property damage

Drone run out of power

Flying a drone with limited power supply in a populated area can pose a serious threat depending on the weight of the drone. If the drone only have a maximum flying time of 10 min and the pilot does not remember to fly the drone to a spot with no people then human safety can be at risk.

The unwanted incident originating from the drone losing power are:

- Human injury
- Property damage

System crash during flight

If the internal system in the drone crashes during flight in populated area it could cause injuries to humans and damage property. The cause for this may be that the drone is of low quality such as a toy drone or the like produced with a very limited budget.

The unwanted incident originating from a system crash during flight are:

- Human injury
- Property damage

Filming without permission

For a bystander the thought of being filmed without knowing it can be terrifying. Mostly this due to the violation of privacy and with a drone it is possible

The unwanted incident originating from filming without permission are:

- Compromise of privacy

Which of the identified direct assets which are being affected by the unwanted incidents are listed below:

- **Human safety**

  HS Human injury
- **Property safety**

  PS Property damage
- **Human privacy**

  HP1 Compromise of bystander privacy

The table below summarise the threats, unwanted incidents and their source for each direct asset.

Unwanted Incident	Threat	Source
Human safety		
HS	Insufficient competencies	Pilot
HS	Drone run out of power	No power on battery
HS	System crash during flight	System failure
Property safety		
PS	Insufficient competencies	Pilot
PS	Drone run out of power	No power on battery
PS	System crash during flight	System failure
Human privacy		
HP1	Filming without permission	Pilot

Table 5.3: The unwanted incidents, threats and source which can affect the Direct Assets.

Identification of controls

For ordinary people there exists no legal controls to handle the identified threats other than the legislation in the country where the incident occurred.

Identification of vulnerabilities

For threats regarding safety the following vulnerabilities are to be considered:

Poor quality technology If the drone is of a poor quality then there is a greater chance of it crashing

Unstable connection In case the drone do not have a return to starting point mechanism then it could crash.

Pilot has Insufficient training For inexperienced pilots flying in a populated area there is a chance for the drone fly into someone.

Pilot has limited technological knowledge If the drone is not calibrated properly then the drone could potentially crash.

However for threats against privacy it is more difficult to identify where the vulnerabilities are located; is it the recklessness of the pilot or perhaps the lifestyle of the bystanders. For some cases it might be considered to be both such as if the pilot is filming into the neighbors backyard where he/she is sunbathing naked. This is a subject which will not be covered here but are open for further discussion.

Identification of consequences

The consequence of people getting injured can be anything from minor scratches to more serious injuries such as concussions, flesh wounds and in worst cases, the injured person losing his life. This depends largely on how much the drone weighs and how unfortunate the crash is. The consequences of damaging property will in worst case render the property unusable depending on the fragility of the property.

By filming bystanders without them knowing the pilot is able to get footage of their private matters include how they live, private doings, etc.. In worst case this could lead to psychological problems for the bystanders depending on the content of the footage and whether it is published in social media or other sites on the Internet. Furthermore by filming the bystanders on their private property the pilot may also be able to analysis the behavioral patterns of the bystanders which can be used in break-ins.

5.2.4 Visualization of identified risks using CORAS

The findings from the Risk identification can be visualized by using the CORAS tool. More precisely the findings from the Asset identification, Threat identification and Vulnerability identification are used to create Threat diagrams. Four diagrams are going to be made:

1. A HTA diagram showing the risks having the pilot a source
2. A HTD diagram showing the risks having an active attacker as source
3. A HTD diagram showing the risks having a passive attacker as source
4. A NHT diagram showing the risks having parts of the system as a source.

HTA diagram

On Fig. 5.4 is shown the threats, unwanted incident, vulnerabilities and affected assets involved in the risks originating from the pilot.

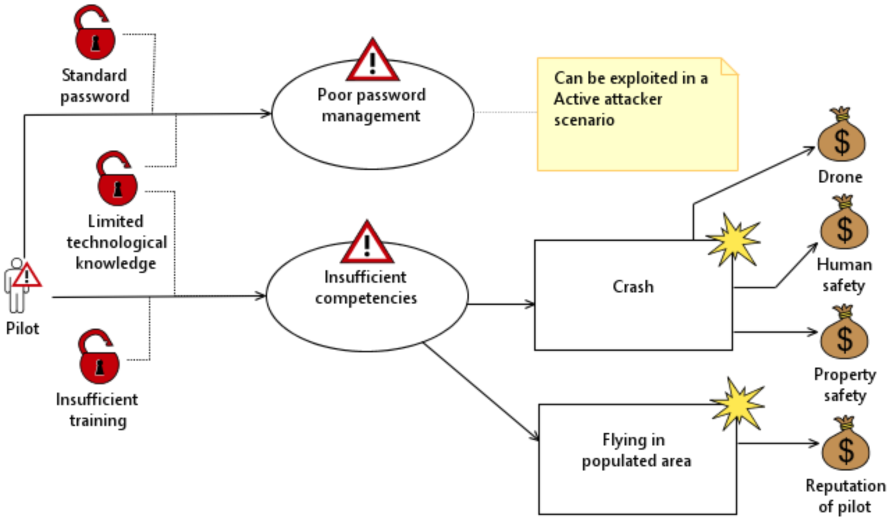


Figure 5.4: A CORAS Threat diagram showing the vulnerabilities, threats, unwanted incidents and affected assets for a HTA source

HTD diagram

On Fig. 5.5 and Fig. 5.6 the threats, unwanted incident, vulnerabilities and affected assets are shown for risks either from a active or passive attacker.

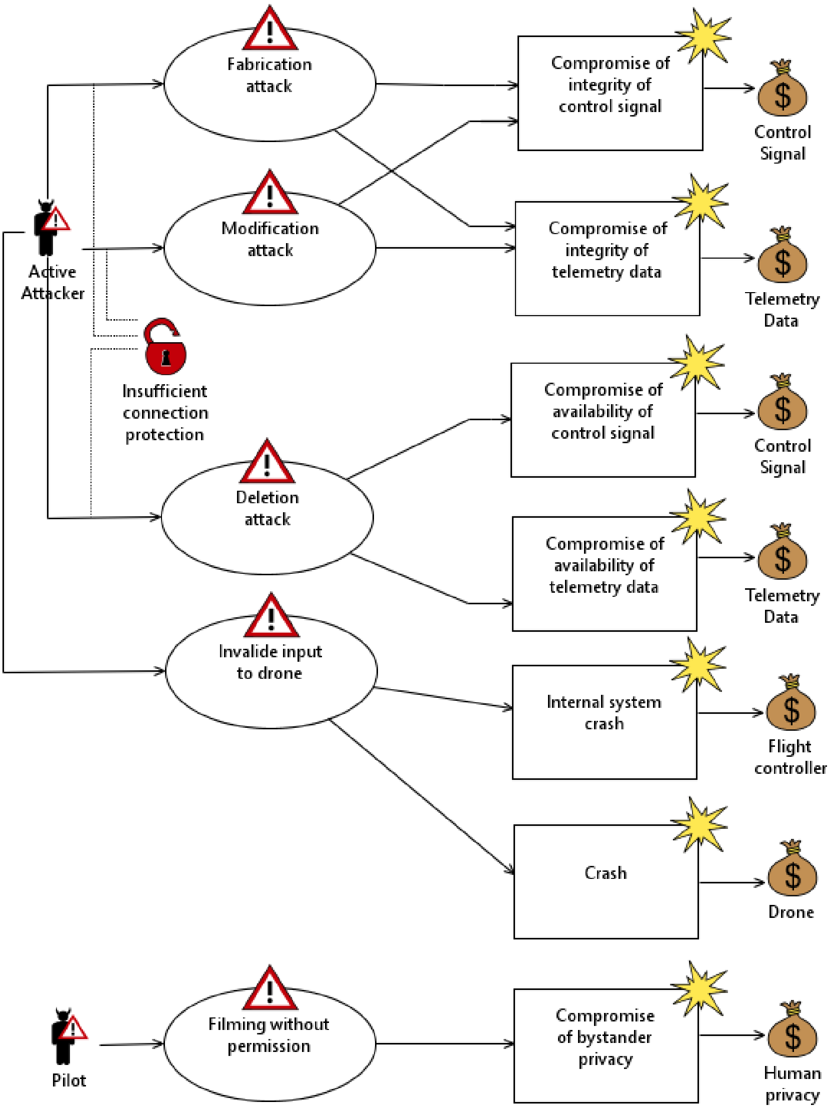

Fabrication attack
Modification attack
Active Attacker
Insufficient connection protection
Deletion attack
Invalide input to drone
Pilot
Filming without permission
Compromise of integrity of control signal
Compromise of integrity of telemetry data
Compromise of availability of control signal
Compromise of availability of telemetry data
Internal system crash
Crash
Compromise of bystander privacy
Control Signal
Telemetry Data
Control Signal
Telemetry Data
Flight controller
Drone
Human privacy

Figure 5.5: A CORAS Threat diagram showing the vulnerabilities, threats, unwanted incidents and affected assets for a active HTD source

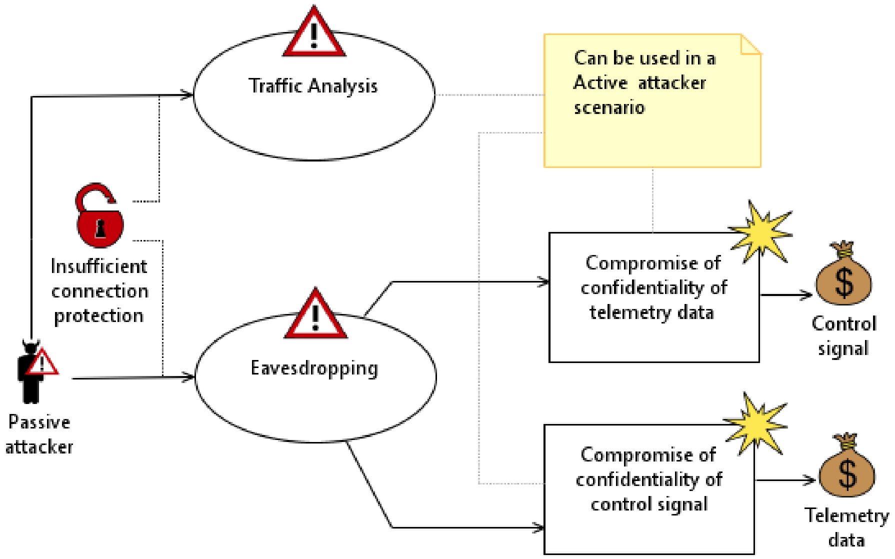

Traffic Analysis
Can be used in a Active attacker scenario
Insufficient connection protection
Compromise of confidentiality of telemetry data
Control signal
Eavesdropping
Passive attacker
Compromise of confidentiality of control signal
Telemetry data

Figure 5.6: A CORAS Threat diagram showing the vulnerabilities, threats, unwanted incidents and affected assets for a passive HTD source

NHT diagram

On Fig. 5.4 is shown the threats, unwanted incident, vulnerabilities and affected assets involved in the risks originating from the system.

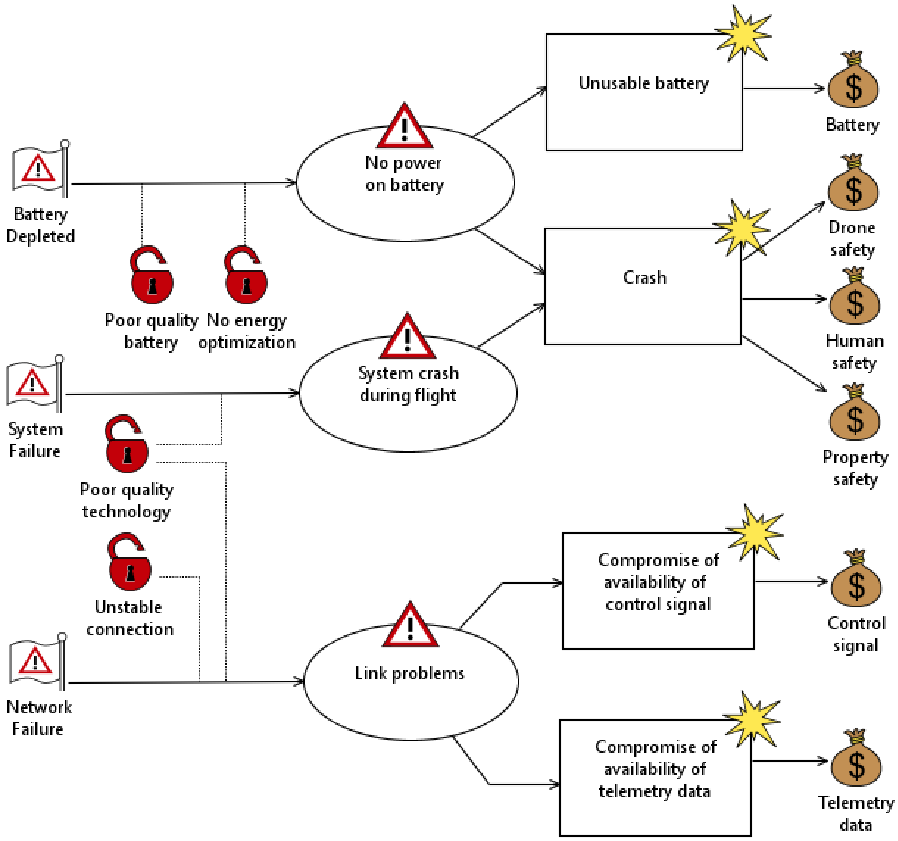


Figure 5.7: A CORAS Threat diagram showing the vulnerabilities, threats, unwanted incidents and affected assets for a NHT source

5.3 Risk Analysis

Now that the risks have been identified the impact and likelihood should be identified for each of the threats. In the table below estimates are made for each of the identified threat regrading their impact and likelihood with the impact rated from the perspective of the stakeholders. To identify each threat and the affected stakeholder the ID is made up from the first letter of the stakeholder and a number.

ID	**Threat**	**Impact**	**Likelihood**
Drone			
D0	Battery depleted	Medium	Medium
D1	Invalid input	Medium	Low
Pilot			
P0	Insufficient competencies	Medium	High
P1	Poor password management	High	Very High
P2	Drone looses power	Medium	Medium
P3	System crash during flight	Medium	Low
P4	Drone link problems	Very High	Low
P5	Eavesdropping	Low	High
P6	Traffic analysis	Low	High
P7	Fabrication attack	Very High	Medium
P8	Modification attack	Very High	Low
P9	Deletion attack	Very High	Medium
Bystander			
B0	Human injury	High	Low
B1	Property damage	Medium	Medium
B2	Filming without permission	Very High	High

Table 5.4: The identified threats for each of the stakeholders with impact and likelihood rating

5.4 Risk Evaluation

The estimated threat impacts and likelihoods for each stakeholder can now be located in the table created in the Context establishment.

		Likelihood				
		Very Low	Low	Medium	High	Very High
Impact	Very Low					
	Low				P5, P6	
	Medium		D1, P3	D0, P2, B1	P0	
	High		B0			P1
	Very High		P4, P8	P7, P9	B2	

Table 5.5: Risk Matrix

In the table it should be noted that none of the threats identified are considered to be low-priority risks, 11 threat are medium-level risk and four threat are high-level risks. The high-level risks include:

- Poor password management,
- Fabrication attack,
- Deletion attack, and
- Filming without permission

where the first three of them concern the pilot and the last concern the by-standers.

Chapter 6

Model Experimentation

6.1 Method

There exists several method and approaches one could take in order to test the security mechanisms implemented in a specific drone model. The following options are the methods considered for use in this project.

6.1.1 Sensor specific attacks

As mentioned in the analysis section of this thesis it could be possible to utilize sensor specific attacks, for example GPS spoofing if a drone navigates using GPS. However, this was not looked further into, instead the focus is directed towards attack vectors on the control signal.

6.1.2 Replaying a control signal

One of the most simple methods is the replay attack. If the drone is not secured against replay attacks one could record the radio signals coming from the drone controller and without trying to decipher it, replay it at a later time to gain the same effect as the original signal was sent to do. In theory the way to do it is to identify the frequency on which the communication between the drone itself and the drone's controller is transmitted. Once the frequency is located one would have to wait for the signal to be transmitted from the drone controller to the drone and using a radio record and save the signal. At a later point the saved signal can be transmitted with the radio and while the drone have no protection against it, is active and turned on, in range and on the same frequency it should be susceptible to the attack and perform the same action as the original signal sent from the authentic controller earlier.

6.1.3 Fabrication of control signal

Perhaps the most effective method is to try and replicate the control signal. If successful it means that a total takeover is possible. If it is possible to reverse engineer the messages between the drone itself and the controller to discover what actually is sent back and forth one could craft his own messages and send them to the drone as if it was from the controller. This method however, may be the most difficult as it requires knowledge of how radio signals are working, specific details about frequency, modulation, bandwidth and other potential unknown factors. It also requires access to some equipment capable of both receiving radio signals and transmit them. Receiving radio waves is needed when trying to reverse engineer a radio signal to observe and analyze it. It is also needed if the drone and the controller uses a connection oriented protocol meaning that they keep sending signals to each other at a certain interval to ensure there's still a connection between the two. Sending radio signals is required when fabricated command is to be sent. Sometimes it is needed to be able to send and receive simultaneously depending on the drone model and the protocol it uses. A device that does both is called a transceiver.

6.1.4 Spoofing

If the signalling system between the drone and drone controller requires a continuous connection in order to work a replay attack will probably not work. Other methods are then needed. Having reverse engineered the protocol used in the communication scheme between the drone and drone controller it should be possible to initiate the handshake from a transceiver radio pretending to be the drone controller. The down side of spoofing is that it is really hard to do properly. Finding out exactly what to send when certain conditions are met and signals received and in the right order and time delay requires a lot of work and patience to figure out and reverse engineer.

6.1.5 WiFi specific attacks

As the most popular drones communicates between itself and the drone controller over radio waves at 2.4GHz frequency, some drone models may use the WiFi protocol. If WiFi is in fact used for communicating control signals it could be vulnerable to specifics exploits that specifically targets WiFi.

6.2 Proof of concept: Replay attack

Performing a replay attack is relatively simple given the right tools. As a proof of concept a simple replay attack was performed locally on a test machine sending UDP packets. Tools used:

- Netcat [25]
- Wireshark [26]
- Tcpreplay [27]

Scripts are written in Bash and Python. The Python scripts are used to encrypt and decrypt text with AES-128 in CBC mode, the recommended method by NIST [22, PR:7.1], with the key

```
    Crypto is funny!
```

and the initialization vector

```
    IV is important!
```

as seen in the two scripts found in Listing 1 and Listing 2.

The bash scripts found in Listing 3 and Listing 4 are used to send UDP packets and continuously listen for incoming ones accordingly. The send script takes a string from stdin, runs it through the Python script to decrypt it and encode it as hexadecimal. It then uses Netcat to send it over the network in a UDP packet. The receiving script also uses Netcat and listens for incoming UDP on the same port. In this example, port 6666 is used. When receiving a packet it runs it through the Python script to decode the content from hexadecimal and decrypt it using the same cryptographic key and initialization vector used the encrypt it. It then just prints the string and it should be the same string as entered on the sending side. The string was successfully send over the network, encrypted so the content was unreadable.

If an attacker were to place himself between the two devices communicating he could intercept the packet in an eavesdropping attack as in Fig. 4.5. Even though the content is encrypted as seen in Fig. B.1, he could still just send the packet at a later time, unedited, to perform a replay attack. If the receiver has not implemented any protection against it, the packet will decrypt to an understandable command as though it was coming from the original sender and the receiver will execute it as such. This means that the attacker could intercept packages, replay them at any time and observe the behavior to figure out the command. He could do this several times to build a load of packets to replay at any time and essentially taking over control without ever breaking the encryption. In this test, using Tcpreplay out the packet intercepted with Wirehark the packet will reach the receiver and he will decrypt it normally, showing of the concept.

One way to protect against replay attacks is by using a nonce or a timestamp that is sent along with the message and is used to verify that this message is new. In Listing 5 and Listing 6 the scripts from before are modified to include a timestamp. If the receiver receives a message where the timestamp is more than 1 second old, the message is rejected. How long one should allow for messages to be accepted depends on the application. In this concept 1 second is sufficient to deter any manual replay attacks with previously intercepted packets.

It is also possible to replay TCP packets but that requires extra work as some of the header fields have to be changed, including the sequence number. If ta TCP packet is desired to be replayed at a later point, the payload may be extracted and put into a new packet and a new 3-way handshake have to be established. This is because TCP is a connection oriented protocol which has focus on having a reliable transmission. UDP is connectionless and have focus on speed.

Replaying other protocols is probably also possible, however the amount of work required depends on the protocol itself and if it is connection oriented or connectionless.

6.3 Equipment

For the real life practical experimentation some equipment is required in order to test the theory.

BladeRF x40

Software defined radio with transceiver capability

2.4GHz WiFi antenna

Antenna mounted on the radio to capture and transmit radio waves on the 2.4GHz frequency

Drone controller

The controller used to transmit and possibly receive data to and from the drone

Drone

The drone itself. What it's all about. Used to monitor radio signals from the controller and if fabricated or replayed signals have an effect

Laptop

A laptop where the software defined radio is connected. The laptop contains a Linux image with the drivers for the BladeRF installed

GNURadio

Software used in the software defined radio. Used to create flow charts describing how to process data either received or or before transmission

Osmocom SDR

Plugin to GNURadio connecting the software defined radio with the drivers for the BladeRF

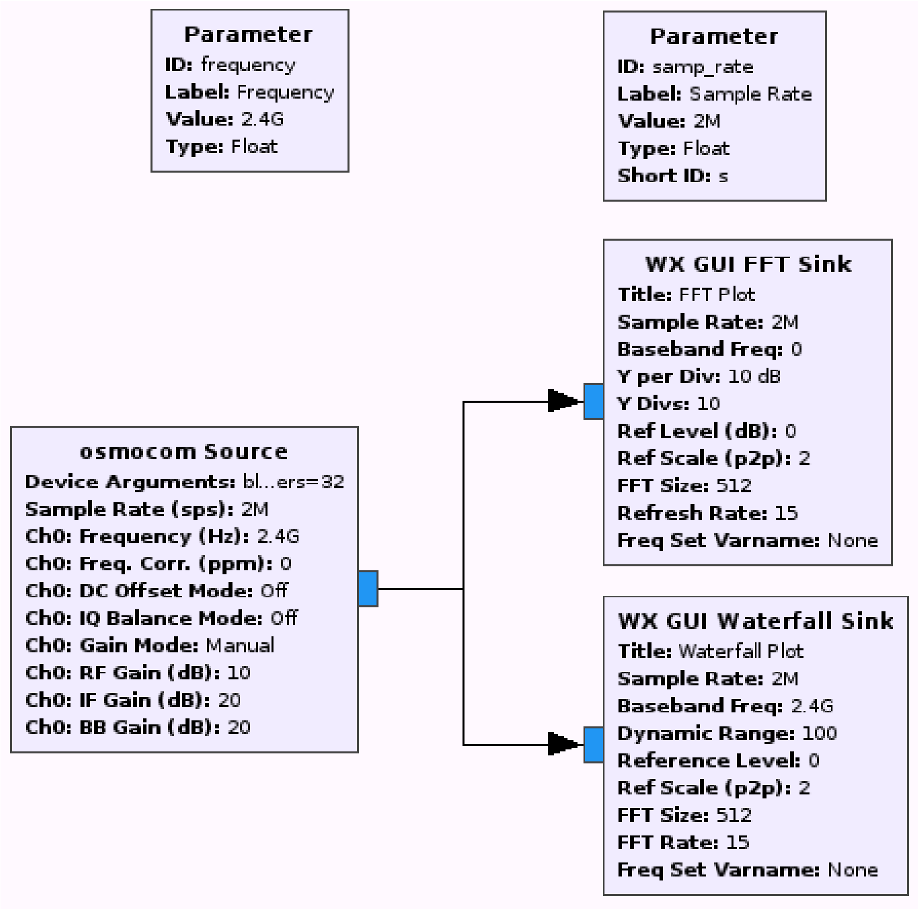
6.4 Experiments

With the equipment in place it was time to perform some real life tests on a recreational drone marketed for consumers. Two different drones were used in this experiment, both manufactures from the list of popular retailed drone models in Table A.1.

The two models used were the Syma X5SW[28] and Hubsan X4[29], both communicating on the 2.4GHz frequency and both RTF-drones.

6.4.1 Software-defined radio

When the equipment was equipped on a Linux machine, the GNURadio software was set up. GNURadio is the software for the SDR and works by creating flowcharts in a drag-and-drop environment.



Parameter
ID: frequency
Label: Frequency
Value: 2.4G
Type: Float

Parameter
ID: samp_rate
Label: Sample Rate
Value: 2M
Type: Float
Short ID: s

osmocom Source
Device Arguments: bl...ers=32
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 2.4G
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 2M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 512
Refresh Rate: 15
Freq Set Varname: None

WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 2M
Baseband Freq: 2.4G
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None

Figure 6.1: GNURadio flowchart connecting the input from the SDR to two different chart types

Figure 6.1 shows the flowchart used to create an FFT plot and a waterfall plot from the input of the BladeRF using the OsmocomSDR plugin and set to listen on the 2.4GHz frequency. The resulting plots can be seen in Fig. 6.2 and Fig. 6.3 respectively.

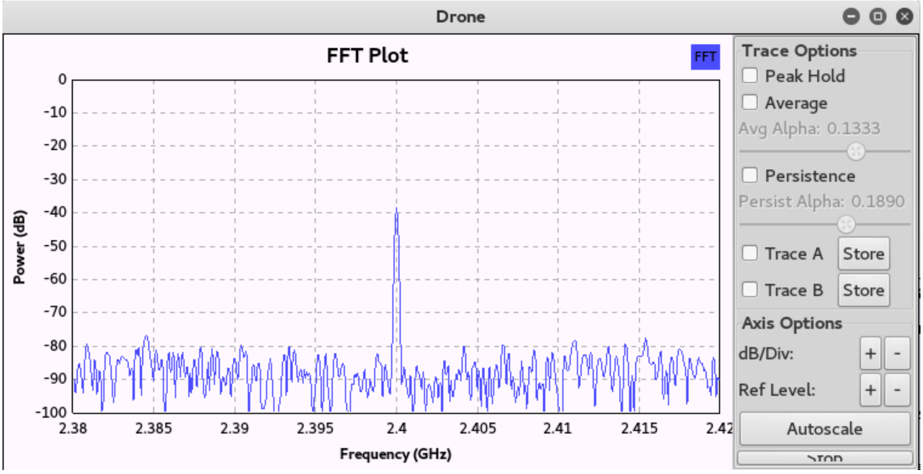


Figure 6.2: FFT plot of the 2.4GHz spectrum

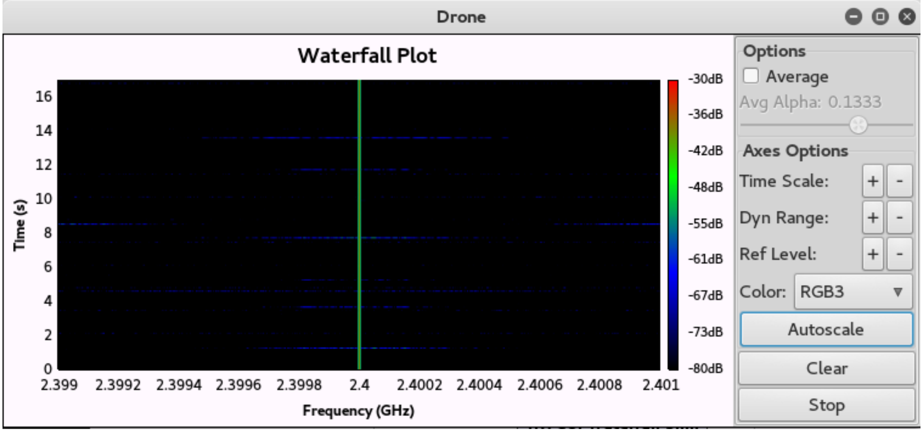
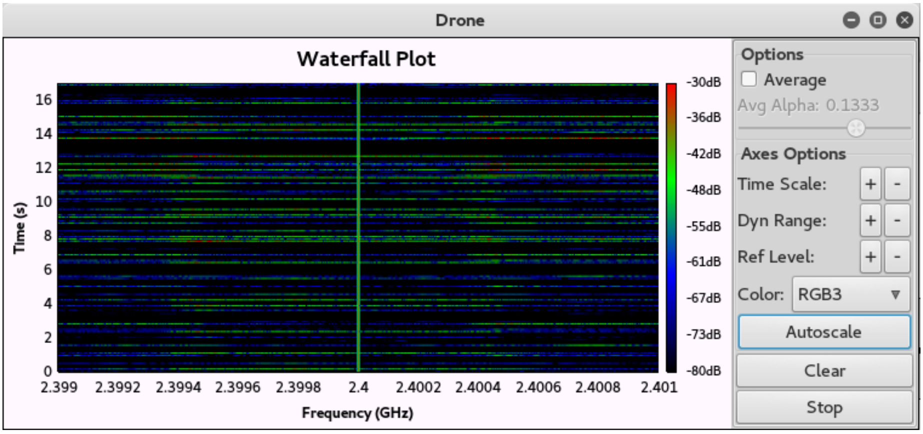


Figure 6.3: Waterfall plot of 2.4GHz spectrum with drone controller turned off

Turning on the drone controller to try and find a signal was different for both drone models. On the Hubsan drone it was clear to see something being transmitted on the 2.4GHz frequency as seen in Fig. 6.4. For the Syma drone however, it was much more difficult. Nothing appeared directly on the 2.4GHz frequency.

Scanning frequencies a little higher such as 2.485GHz showed something being transmitted but as 2.4GHz is an ISM band it could've been a lot of things and not the drone and it's controller specifically. The same frequency did not always yield results, so it is possible that the signal were not from the Syma drone but something else or it is using frequency hopping to shift to less used frequencies in the 2.4GHz band.



Options
□ Average
Avg Alpha: 0.1333
Color: RGB3

Figure 6.4: Waterfall plot of 2.4GHz spectrum with drone controller turned on

As the documentation for both drones are very limited the reverse engineering process involved a lot of trial-and-error and guess work. None of the models described any modulation type, bandwidth or other parameters only the use of the 2.4GHz frequency thus making the process difficult.

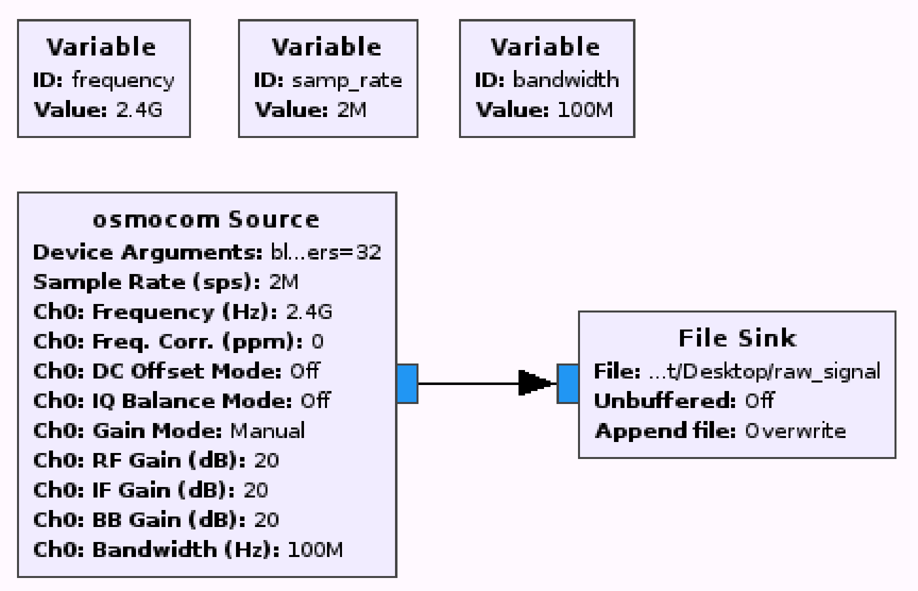
Furthermore as the 2.4GHz frequency is so heavily used it is difficult to isolate a signal from the drone and to know that the signals the radio are picking up are actually from the drone or it's controller and not something else communicating in the same band.

Another obstacle is that both drone models seems to be using some sort of handshake to initiate and maintain the connection between the drone and the drone controller. This complicates the process of reverse engineering as it requires a continuous connection from the BladeRF and to to able to send and receive simultaneously with the right timing and sequences as it appears to be using a connection oriented protocol.

6.4.2 Replay attack

The replay attack is an obvious choice to try out first. There are multiple ways to do this at different points in time depending on what communication part is wanted to be attacked. It could be the setup phase by replaying a previous handshake or simply replaying a previously sent command in an ongoing session.

Constructing the flow graph in GNURadio is a simple matter of taking the raw input signal and saving it to a file as seen in Fig. 6.5.



ID: frequency
Value: 2.4G

ID: samp_rate
Value: 2M

ID: bandwidth
Value: 100M

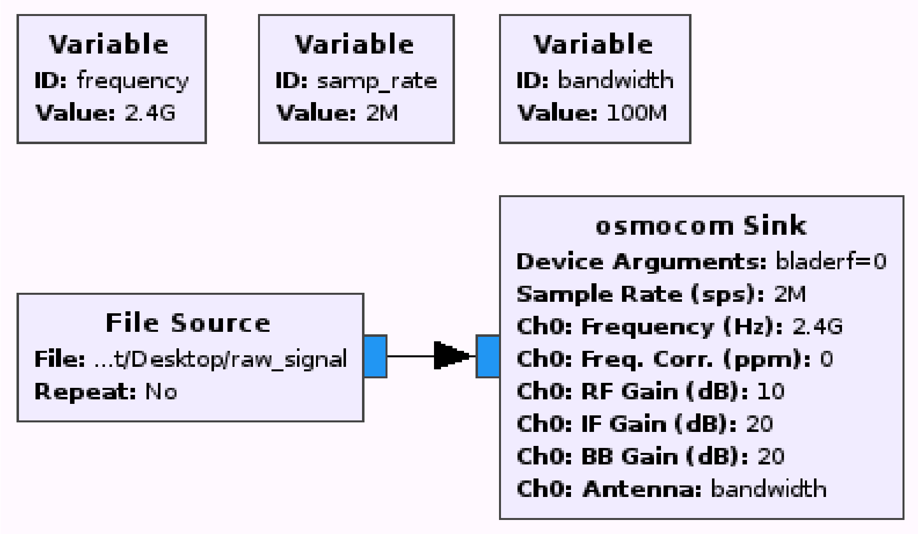
Device Arguments: bl...ers=32
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 2.4G
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 20
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Bandwidth (Hz): 100M

File: ...t/Desktop/raw_signal
Unbuffered: Off
Append file: Overwrite

Figure 6.5: GNURadio flowchart of raw signal received being saved

The raw signal were captured for both the handshake protocol and for general controls of the drone during an already establish session between the drone and the drone controller.

Replaying the signal with GNURadio was as simple as capturing as the saved file now is used as the source and the radio is now used to transmit the signal as seen in Fig. 6.6.



Variable
ID: frequency
Value: 2.4G

Variable
ID: samp_rate
Value: 2M

Variable
ID: bandwidth
Value: 100M

File Source
File: ...t/Desktop/raw_signal
Repeat: No

osmocom Sink
Device Arguments: bladerf=0
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 2.4G
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Antenna: bandwidth

Figure 6.6: GNURadio flowchart of previously saved raw signal being retransmitted

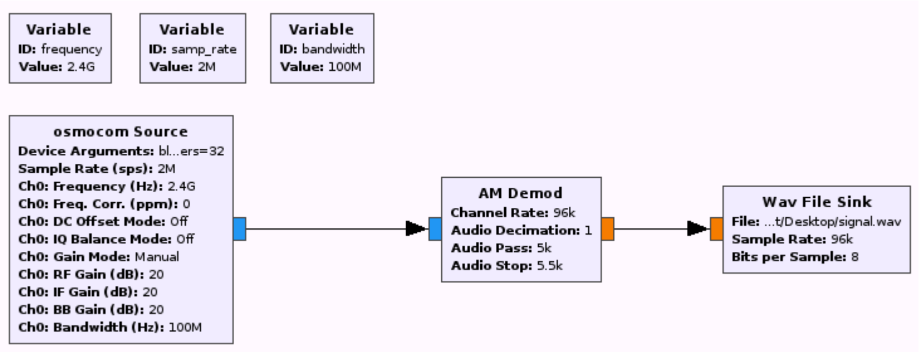
Experiments included both capturing and replaying the initial handshake communication and a command signal in an ongoing connection between the drone and drone controller.

However, as observed earlier the drone and the drone controller seems to use a reliable connection protocol possibly numbering packets thus offering protection from the most basic replay attacks - the ones that just replay the raw signal.

As suspected neither of the replay attacks has any visible effects on the drone. Even the replaying of a command signal in an ongoing connection proved unsuccessful. If a session ID is randomised for every session this attack should at least use the correct ID and format as the connection is still established. It did however not produce any visible effects on the drone thus further strengthening the theory that a reliable protocol that possibly numbers the packets are used. Without completely reverse engineering the signal it seems that a replay attack is not useful in this context.

6.4.3 Analyzing the control signal

Trying to analyse the also proved difficult as the documentation, as mentioned earlier, is very lackluster. Trying different types of demodulation such as FM, AM, PSK, QPSK and GFSK with different parameters the Syma drone did not yield anything that looked like it could be a control signal from the drone.



Variable
ID: frequency
Value: 2.4G

Variable
ID: samp_rate
Value: 2M

Variable
ID: bandwidth
Value: 100M

osmocom Source
Device Arguments: bl...ers=32
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 2.4G
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 20
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Bandwidth (Hz): 100M

AM Demod
Channel Rate: 96k
Audio Decimation: 1
Audio Pass: 5k
Audio Stop: 5.5k

Wav File Sink
File: ...t/Desktop/signal.wav
Sample Rate: 96k
Bits per Sample: 8

Figure 6.7: GNURadio flowchart of signal being AM demodulated and saved in a wave file

However, the Hubsan drone, when amplitude demodulated and saved in a wave file (Fig. 6.7), showed something interesting. Several segments of sequences of little bumps on the wave were revealed, as seen in Fig. 6.8, zoomed in on one of the segments.

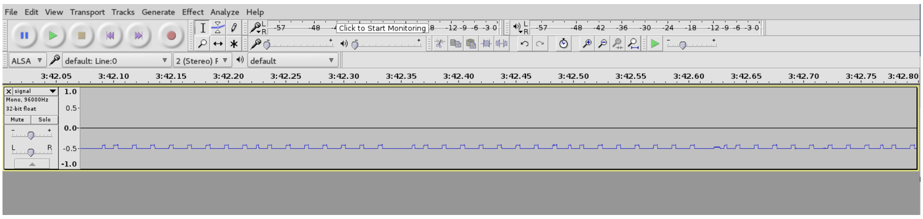


Figure 6.8: Wave file of AM Demodulated signal on the 2.4GHz spectrum with drone controller turned on

It is unknown what this sequence actually is but it could possibly be a bit string where the little bumps represent 1 and no bump represents 0.

But without knowing the actual protocol and connection schema the experiments stops here. Maybe this signal is actually something used by the drone controller, maybe not. This is definitely something that could be looked further into.

At an internet forum of remote control hobbyists, a user have made an initial analysis of the Hubsax drone and it's communication protocol [30]. This verifies the theory of the drone using some sort of handshake protocol to establish and maintain a connection in addition to adaptive channel using. This only adds up to the difficulty of the reverse engineering and hacking of the drone, however given the right know-how, tools and time it indeed seems likely to actually find one or more exploits in security of the Hubsan drone.

6.4.4 WiFi-based attacks

As neither of the drones in possession are WiFi-based it is difficult to actually test some of the possible vulnerabilities. The Syma[28] drone however have a camera that can be mounted on the drone and the way to view the images from the camera is to connect a WiFi access point it creates and open their application on a smart phone.

Authentication

First observation was that the WiFi access point the drone creates is not encrypted, meaning that everyone in proximity can connect to it. When connecting to the access point and starting up the smart phone application a connection is established between the camera and the phone. The camera data is then transmitted via TCP to the phone as seen in Fig. B.2.

De-authentication attack

Performing a de-authentication attack on the drone camera was a simple experiment. Using the command line tool 'aircrack-ng'[31] it was possible to first establish the MAC address and channel of the camera using the following command.

```
airodump-ng wlxe84e062e0d39
```

In this case 'wlxe84e062e0d39' is the name of the wireless network interface put into monitor mode. The name is describing that it's a wireless module and it have appended it's MAC address, however the actual name is not important other than to know the correct network interface top use. In other cases it could have a name like 'wlan0'.

The output will be a live listing of wireless networks nearby, their base station MAC address, channel number, SSID and more information. When the channel number is revealed a dedicated scan on that channel can begin to find the MAC address of connected devices., using the following command.

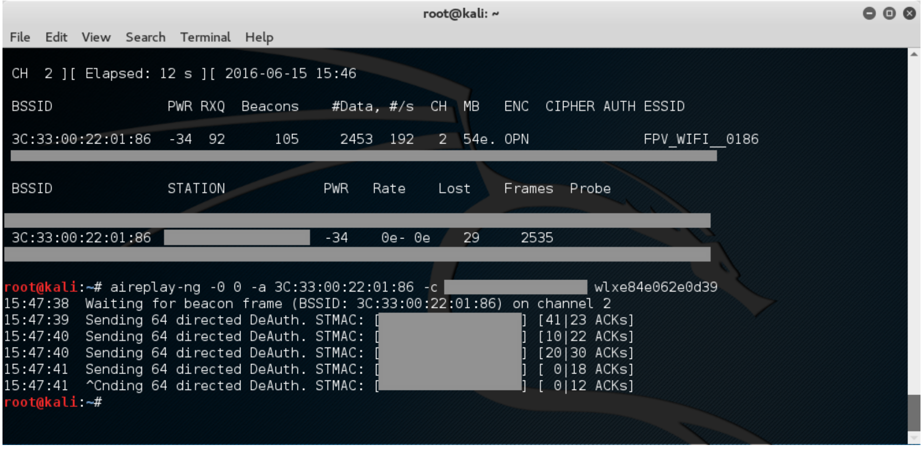
```
airodump-ng -c 2 wlxe84e062e0d39
```

Where the -c parameter is the channel number, in this case 2. The output shows a live listing of found WiFi frames on that particular channel. As shown in the screen shot in Fig. 6.9 the MAC address is found for the access point with SSID of 'FPV_WIFI__0186' and a connected device. Using the MAC address of both base station and connected device, the attack can begin. Using the follow command the de-authentication frames are transmitted.

```
aireplay-ng -0 0 -a 3C:33:00:22:01:86 -c <Device MAC> wlxe84e062e0d39
```

This command continues to transmit de-authentication frames until terminated by the user making the device unable to reconnect as long as the attack is ongoing.

As seen in Fig. 6.9, when launching the attack the the terminal windows will output the current status of the program. As soon as the directed de-authentication frames were sent the mobile application lost connection to the camera on the drone and were thus unable to watch the live images from the camera, proving this attack method successful.



```
CH  2 ][ Elapsed: 12 s ][ 2016-06-15 15:46

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

3C:33:00:22:01:86  -34  92      105     2453  192   2  54e. OPN              FPV_WIFI__0186
[redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

[redacted]
3C:33:00:22:01:86  [redacted]  -34    0e- 0e    29     2535
[redacted]

root@kali:~# aireplay-ng -0 0 -a 3C:33:00:22:01:86 -c [redacted] wlxe84e062e0d39
15:47:38  Waiting for beacon frame (BSSID: 3C:33:00:22:01:86) on channel 2
15:47:39  Sending 64 directed DeAuth. STMAC: [[redacted]] [41|23 ACKs]
15:47:40  Sending 64 directed DeAuth. STMAC: [                 ] [10|22 ACKs]
15:47:40  Sending 64 directed DeAuth. STMAC: [                 ] [20|30 ACKs]
15:47:41  Sending 64 directed DeAuth. STMAC: [                 ] [ 0|18 ACKs]
15:47:41  ^Cnding 64 directed DeAuth. STMAC: [                 ] [ 0|12 ACKs]
root@kali:~#
```

Figure 6.9: De-authentication attack on drone camera WiFi
The MAC address of the phone and other nearby devices have been masked

WiFi-controlled drone

A short experimentation was conducted on a popular drone model, the Parrot AR.Drone 2.0[32]. This drone is fully WiFi-controlled and uses an application on a smartphone to navigate. Furthermore the manufacturer provides an SDK for Linux making navigation and live video feed possible from the Linux computer with a WiFi-enabled network card. It was found that WiFi the drone creates is no password protected leaving it open for anyone to join it. Opening up the SDK made it possible to receive some information from the drone but not control it as it seemed to require some extra steps and be in physical possession of the drone. It was however possible to conduct a de-authentication attack and disconnect the smartphone from the drone.

Chapter 7

Risk treatment and model evaluation

Using the results from Chapter 5 recommendations for treating the risk can be proposed. The recommendations will be based on theory Section 4.4 and the identified controls from Chapter 5. When the treatments have been proposed the created model which include the findings in Chapter 5 and the proposed treatments will be evaluated in relation to real world incidents. The reason for doing this is to find out whether or not the model that has been constructed would be able to detect real life incidents.

7.1 Risk Treatment

As it stands, there are three primary ways a drone get input for navigation as seen in Fig. 3.1:

- The control signal
- Telemetry data
- Sensors

Each input source must be properly protected to prevent unwanted incidents. The identified threats in Chapter 5 and the experimentation performed in Chapter 6 leave us with the following recommendations to properly ensure security in a drone system thus eliminating as many risks as possible and feasible.

As both the control signal and telemetry data is communicated using radios it is essential that the transfer of signals are done in a secure way that preserves both confidentiality, integrity and provides proper authentication.

7.1.1 Confidentiality

Encrypting the signals before transmission will ensure confidentiality but it is important to use both a strong key and a strong encryption algorithm. The National Institute of Standards and Technology (NIST) recommends using the AES-128 algorithm which is considered amongst the best and strongest symmetric key encryption algorithms. The mode of operation to use is dependent on what is desired. If only confidentiality is wanted then the Cipher-Block-Chaining (CBC)[22, PR:7.1] mode is recommended. If both confidentiality and authenticity is wanted then the Galois/Counter-Mode (GCM)[22, PR:7.3] is recommended.

Key exchange

To ensure confidentiality the key exchange between the drone and the controller should be managed properly such that the key will remain a secret between the drone and the controller. This can for instance be done by integrating a security module into the drone or by using the RSA encryption algorithm. These solutions however would be to costly both in terms of implementation cost and power consumption. For this reason a simpler method is recommended by using a cable to transfer the key preferably generated by the controller to save energy in the drone. Additionally it is recommended to use a cryptographically secure pseudo-random number generator to generate the encryption key.

7.1.2 Integrity

As we want to ensure integrity we recommend using AES with the GCM mode of operation as it ensures authenticity and integrity. GCM works by in addition to encryption the signal it adds an authentication code along the ciphertext and initialisation vector. The authentication code is used to create an authentication tag that is used as a method of validating the integrity of the message.

The integrity of sensors need proper integrity. Invalid data and malformed data should be discarded. The system also needs to compare data with previous data in order to identify and ignore outlier data - whether it is a measuring error or sensor spoofing. Spoofing sensors can be difficult to protect against but is possible given enough resources, for example GPS spoofing countermeasures[33].

7.1.3 Availability

To ensure availability it is important to distinguish between whether the drone is unavailable internally or externally. Being unavailable externally can happen if for some reason the signal never reaches the drone, for example by a deletion attack, interference on the frequency, or the drone being out of range. Internally unavailability can happen if the drone does not have enough resources to process the messages either because of denial-of-service attacks, improper handling of invalid data causing a system crash, or batter depletion.

To ensure the external availability we recommend using mechanisms to detect crowded channels and dynamically allowing changing this. Using a frequency hopping spread spectrum the drone and the drone controller can change channels in order to prevent unavailability. Frequency hopping algorithms such as AFHDS2 is already used by several drone manufactures but not all.

Internal availability is ensured by having a proper message handling. The system should check for invalid data and correct formatting before doing anything with it, such as storing in the buffer. This prevents packet flooding and malformed packets causing buffer overflow and system crashes. Furthermore the system should include a battery monitor that check the battery charge. If the drone system is running low on battery, does not have more space in the buffer, or lose connection to the controller it should always have a fail safe to land safely instead of blindly trusting and storing the received data - be it from the drone controller, telemetry module or the sensor array.

7.1.4 Authenticity

The GCM mode of operation ensures authenticity on the transmitted signals but can still be vulnerable to replay attacks. To combat this every message should include parts to prevent this. It can either be a time stamp that the receiving unit validates that it is a new message - requires the unit to have an accurate or synchronised clock. Another solution is to include a nonce - a number only used once so the unit can know that the message is new - requires storage space for used numbers.

Looking at actual real life incidents it becomes clear that most of these attacks are due to poor security policy.

List of known real life attacks:

- GPS spoofing [17][34]
- No encryption [35][36]
- No authentication [36][37]
- Brute forcing weak password [38]
- Cracking weak encryption in telemetry module [39]
- ID spoofing [37]
- Packet flooding [40]
- Large packets causing stack overflow [40]
- Packet injection [40]
- Jamming [41]
- De-authentication [Section 6.4.4]

Evaluating the attacks against our model the leads to the following results:

GPS spoofing

Would be 'catched' by the model as a Fabrication attack. Invalid data should be detected and discarded per Section 7.1.2

No encryption

Would be ’catched’ by the model as the vulnerability ’Insufficient connection protection’. Strong encryption is required per Section 7.1.1

No authentication

Would be ’catched’ by the model as the vulnerability ’Insufficient connection protection’. Authentication should always be required per Section 7.1.4

Brute forcing weak password

Would be ’catched’ by the model as the vulnerability ’Poor password management’. Strong encryption key is required per Section 7.1.1

Cracking weak encryption in telemetry module

Would be ’catched’ by the model as the vulnerability ’Insufficient connection protection’. Strong encryption key is required per Section 7.1.1

ID spoofing

Would be ’catched’ by the model as a Fabrication attack. Authentication should always be required per Section 7.1.4

Packet flooding

Would be ’catched’ by the model as a Deletion attack. When the buffer is full because of too many requests the drone should not cause a system crash but land safely per Section 7.1.3

Large packets causing stack overflow

Would be ’catched’ by the model as a Fabrication attack. Too large packets should not cause a system crash but cause the drone to land safely per Section 7.1.3

Packet injection

Would be ’catched’ by the model as a Fabrication attack. Authentication should always be required per Section 7.1.4 and invalid data should be discarded per Section 7.1.3

Jamming

Would be 'catched' by the model as a Deletion attack. Without contact to the controller, the drone should land safely per Section 7.1.3

De-authentication

Would be 'catched' by the model as a Deletion attack. Without contact to the controller, the drone should land safely per Section 7.1.3

It should be noticed that not all real life attacks are 'catched' by the model as being threat but instead vulnerabilities. Despite not being the original intention the 'catching' of vulnerabilities is not a problem as they should be attended never the less since they can be exploited by the 'catched' threats.

Chapter 8

Discussion

As the model now have been established and evaluated against real-life attacks we can see that these vulnerabilities would have been discovered. There are however some drawbacks to this model. First of all the model's only goal to ensure security - not safety and privacy. These are only ensured indirectly from attackers through security of the drone. When the pilot himself is malicious on have a purpose of violating the safety or privacy of others, this model is not sufficient. The only way to prevent illegitimate uses of a drone is through legislation. The adopted legislation in Denmark have good opportunity to ensure safety and privacy by dissuade possible pilots wishing to threaten the safety and/or privacy of others. This of course will not be a complete solution as in some cases the pilot might do it anyway.

Through the work with the ISO 27005 method it was found to be insufficient in relation to how the drone environment was constructed which meant that the method had to be adapted to handle multiple stakeholders. The usage of the CORAS tool in the risk assessment process has turned out to be a good idea, as it helped to increase the understanding of the adapted ISO 27005 method. The CORAS method was not used however so it is hard to tell whether it would have been a preferred choice instead.

The model is proved to offer better security but at a cost. Offering confidentiality, integrity, and availability through the means of our model is not free. Whether the cost is extra power consumption, or extra implementation cost or extra components making the drone heavier, it is a balance the manufacturer must consider. Adding a secure module to store and generate keys is probably the most secure solution, but an expensive one in both cost and power consumption which is why we recommend other methods. Adding an encryption module is again extra implementation cost and the whole encryption-decryption and integrity checking can add delay which is undesired in a real-time communication session plus use extra power from the drones already limited battery. As for the AES encryption, many modern processors today have an integrated AES instruction set that makes it more efficient. Using the GCM mode of operation with AES is also a very efficient and fast mode as it can be parallelised.

We don't have a recommendation on the communication protocol itself as one may be just as good as another. Only recommendation is to use connection oriented protocol as reliability is always desired and thus the drone can detect if the signal to the controller is lost. In case of lost connection the drone should land safely so an established connection is preferred.

Whether to use RF, WiFi, or other communication technologies is also a matter of preference. WiFi is a proven reliable standard that requires no extra hardware than a laptop computer or a smartphone. Thus the manufacturer can save on the production cost as they does not have to include a drone controller - the user already have one: his smartphone. Using WiFi instead of RF however leaves it open to WiFi specific attacks - for example de-authentication attacks. As WiFi is the de-facto standard for wireless Internet communication it have many known attack vectors - some of them hard to protect against. And as WiFi is in every laptop computer and smartphone today, an attacker would need no extra equipment to perform attacks as he already have a WiFi network card onboard his device. If using RF an attacker would need extra equipment, which costs money, and more know-how in the field of wireless communication than a command line tool in Linux requires. RF is not more secure than WiFi but adds an extra layer of complexity which may deter some attackers from attacking.

As always when talking about information security, securing systems is a trade-off between security and convenience. The user does not want to go through a long process of authentication and other setup every time he wants to fly his drone - but on the other hand he does not want others to take over the control of it. The other trade-off is the implementation of the security measures - the cost and power it requires when the manufacturer is competing against other companies on price and flying time. It is a fine balance that is have to be considered carefully.

Chapter 9

Conclusion

By using the risk management method ISO 27005 as a template a model was created assessing the topics of security, safety and privacy in a drone environment. This have been done through distinguishing the stakeholders, being the drone, the pilot and the bystanders, in the environment in order to create a more accurate model. To improve the understanding of the mutual influence between the identified assets and the courses of the risks, the tool from the risk assessment method CORAS, has been used. The model produced showed that there could exist several risks which needed to be handled in the drone environment.

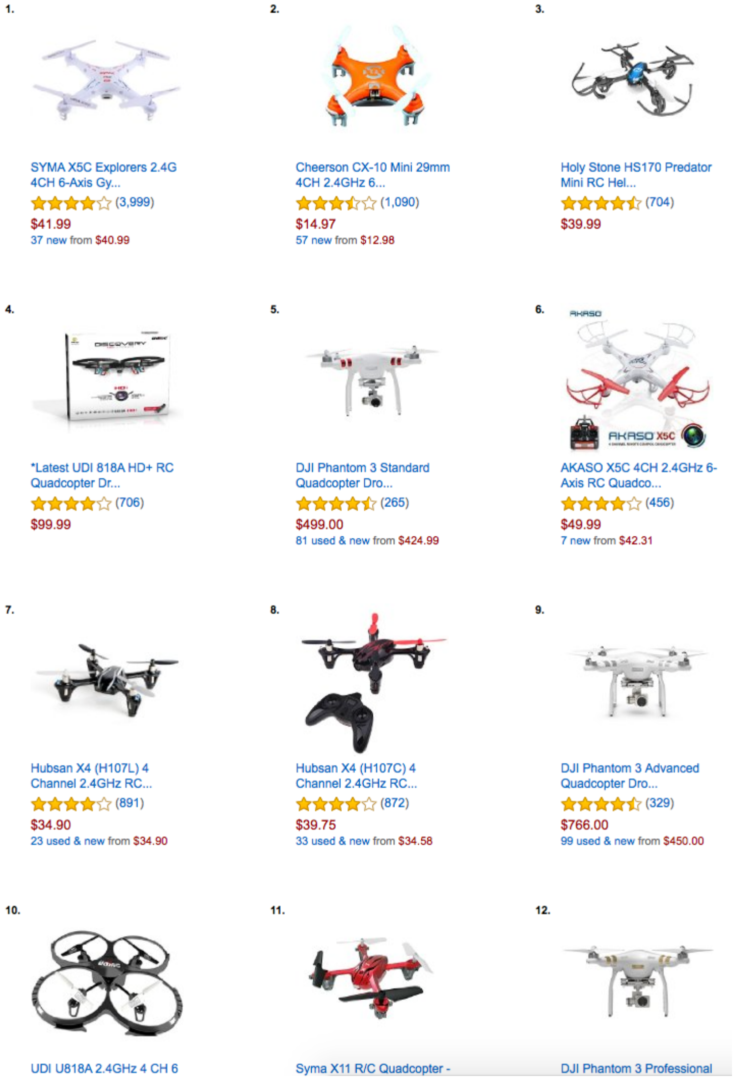
A series of experiments was then conducted in order to find any vulnerabilities and threat against drones. These experiments showed that drones using RF for communication is more complex as it requires more know-how on the topic of wireless communication and extra equipment, while WiFi based drones are more easily attacked with simple tools. Common for all drones is that security does not seems to be high on the list of priorities and some manufactures outright have no security implemented. If the drone popularity continues to rise this is certainly to cause more attacks in the future potentially compromising our safety and privacy.

Finally risk treatments has been proposed focusing on the identified risks in the model with a primary focus on the area of security. Real life drone attacks, including the conducted experiments, where then examined and identified in the model, and treatment plans to handle the real life risk on basis of the proposed risk treatments were then recommended.

It was found that the model was able to 'catch' the real life attacks which supported the reliability of the model not just theoretically but also from a practical point of view.

Appendix A

Popular drone models



1.

SYMA X5C Explorers 2.4G 4CH 6-Axis Gy...

★★★★☆ (3,999)

$41.99

37 new from $40.99

2.

Cheerson CX-10 Mini 29mm 4CH 2.4GHz 6...

★★★⯪☆ (1,090)

$14.97

57 new from $12.98

3.

Holy Stone HS170 Predator Mini RC Hel...

★★★★⯪ (704)

$39.99

4.

*Latest UDI 818A HD+ RC Quadcopter Dr...

★★★★☆ (706)

$99.99

5.

DJI Phantom 3 Standard Quadcopter Dro...

★★★★⯪ (265)

$499.00

81 used & new from $424.99

6.

AKASO X5C 4CH 2.4GHz 6-Axis RC Quadco...

★★★★☆ (456)

$49.99

7 new from $42.31

7.

Hubsan X4 (H107L) 4 Channel 2.4GHz RC...

★★★★☆ (891)

$34.90

23 used & new from $34.90

8.

Hubsan X4 (H107C) 4 Channel 2.4GHz RC...

★★★★☆ (872)

$39.75

33 used & new from $34.58

9.

DJI Phantom 3 Advanced Quadcopter Dro...

★★★★⯪ (329)

$766.00

99 used & new from $450.00

10.

UDI U818A 2.4GHz 4 CH 6

11.

Syma X11 R/C Quadcopter -

12.

DJI Phantom 3 Professional

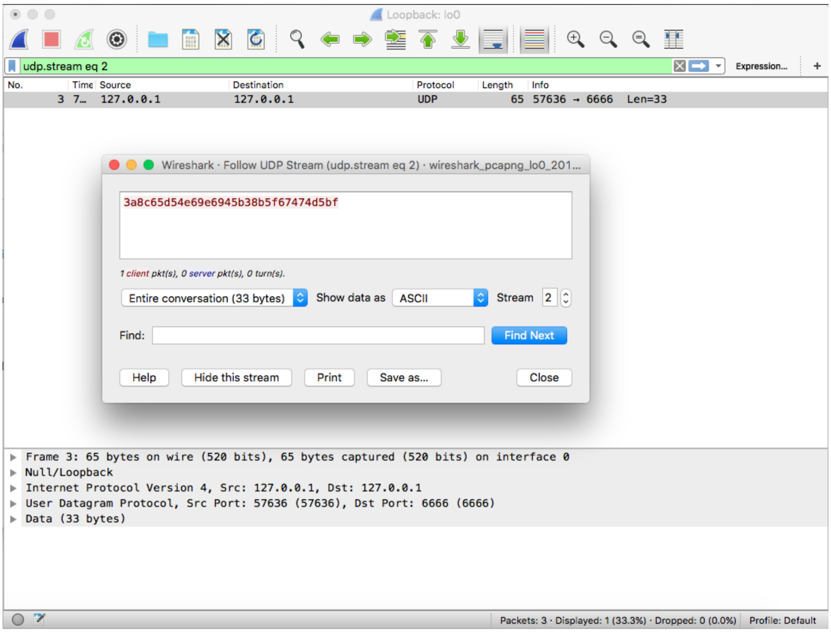
Figure A.1: Drone best sellers on Amazon (Date: March 4 2016) `http://www.amazon.com/Best-Sellers-Toys-Games-Hobby-RC-Helicopters/zgbs/toys-and-games/166591011`

#	Drone	Price	Frequency	Camera	Live	Fly time	Weight
1	SYMA X5C	$41.99	2.4GHz (RF)	Yes	Yes	7 min	953 g
2	Cheerson CX-10	$14.97	2.4GHz (RF)	No	-	4-8 min	91 g
3	Holy Stone HS170	$39.99	2.4GHz (RF)	No	-	6-8 min	408 g
4	UDI Discovery HD+	$99.99	2.4GHz (WiFi)	Yes	Yes	7-9 min	130 g
5	DJI Phantom 3 Standard	$499	2.4GHz (WiFi)	Yes	Yes	25 min	1216 g
6	AKASO X5C	$49.99	2.4GHz (RF)	Yes	No	5-7 min	82 g
7	Hubsan X4 (H107L)	$34.90	2.4GHz (RF)	No	-	9 min	590 g
8	Hubsan X4 (H107C)	$39.75	2.4GHz (RF)	Yes	No	7 min	499 g
9	DJI Phantom 3 Advanced	$766	2.4GHz (WiFi)	Yes	Yes	23 min	1280 g
10	UDI U818A	$75.55	2.4GHz (RF)	Yes	No	7-9 min	119 g

Table A.1: The 10 most sold hobby drones on Amazon.com (Date: March 4 2016), with specifications from `drones.specout.com`

Appendix B

Screenshots



udp.stream eq 2

```
No.  Time Source      Destination  Protocol Length Info
   3 7…   127.0.0.1   127.0.0.1    UDP          65 57636 → 6666  Len=33
```

Wireshark · Follow UDP Stream (udp.stream eq 2) · wireshark_pcapng_lo0_201...

```
3a8c65d54e69e6945b38b5f67474d5bf
```

1 client pkt(s), 0 server pkt(s), 0 turn(s).

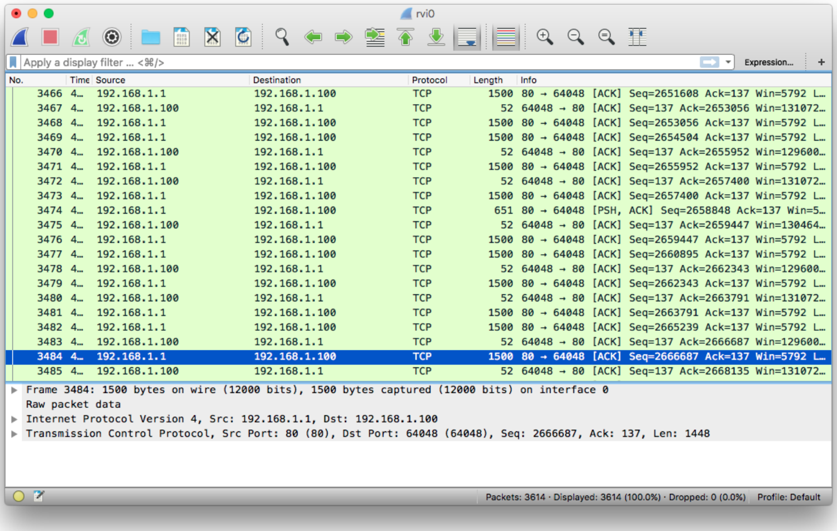
Entire conversation (33 bytes) Show data as ASCII Stream 2

Find:

```
▶ Frame 3: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
▶ Null/Loopback
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 57636 (57636), Dst Port: 6666 (6666)
▶ Data (33 bytes)
```

Packets: 3 · Displayed: 1 (33.3%) · Dropped: 0 (0.0%)   Profile: Default

Figure B.1: Wireshark captured UDP packet with encrypted payload



No.	Time	Source	Destination	Protocol	Length	Info
3466	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2651608 Ack=137 Win=5792 L…
3467	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2653056 Win=131072…
3468	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2653056 Ack=137 Win=5792 L…
3469	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2654504 Ack=137 Win=5792 L…
3470	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2655952 Win=129600…
3471	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2655952 Ack=137 Win=5792 L…
3472	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2657400 Win=131072…
3473	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2657400 Ack=137 Win=5792 L…
3474	4…	192.168.1.1	192.168.1.100	TCP	651	80 → 64048 [PSH, ACK] Seq=2658848 Ack=137 Win=5…
3475	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2659447 Win=130464…
3476	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2659447 Ack=137 Win=5792 L…
3477	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2660895 Ack=137 Win=5792 L…
3478	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2662343 Win=129600…
3479	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2662343 Ack=137 Win=5792 L…
3480	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2663791 Win=131072…
3481	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2663791 Ack=137 Win=5792 L…
3482	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2665239 Ack=137 Win=5792 L…
3483	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2666687 Win=129600…
3484	4…	192.168.1.1	192.168.1.100	TCP	1500	80 → 64048 [ACK] Seq=2666687 Ack=137 Win=5792 L…
3485	4…	192.168.1.100	192.168.1.1	TCP	52	64048 → 80 [ACK] Seq=137 Ack=2668135 Win=131072…

```
▶ Frame 3484: 1500 bytes on wire (12000 bits), 1500 bytes captured (12000 bits) on interface 0
  Raw packet data
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 64048 (64048), Seq: 2666687, Ack: 137, Len: 1448
```

Packets: 3614 · Displayed: 3614 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Figure B.2: TCP connection between drone camera and smartphone

Appendix C

Listings

```python
from Crypto.Cipher import AES
import sys

data = sys.argv[1]

# Add padding
length = 16 - (len(data) % 16)
data += chr(length)*length

obj = AES.new("Crypto is funny!", AES.MODE_CBC, "IV is important!")

ciphertext = obj.encrypt(data)

print ciphertext.encode(’hex’)
```

Listing 1: Encryption - Python script

```
import sys
from Crypto.Cipher import AES

data = sys.argv[1].decode(’hex’)

obj = AES.new("Crypto is funny!", AES.MODE_CBC, "IV is important!")

cleartext = obj.decrypt(data)
pad = ord(cleartext[-1])

print cleartext[:-pad]
```

Listing 2: Decryption - Python script

```
while read line
do
        enc=$(python encrypt.py "$line")
        echo $enc | nc -4u -w1 127.0.0.1 6666
done
```

Listing 3: Send - Bash script

```
while true
do
        response=$(nc -w 1 -vvul 0.0.0.0 6666 2>&1)
        python decrypt.py $response
done
```

Listing 4: Receive - Bash script

```
while read line
do
        timestamp=$(date +%s)
        data="$timestamp:$line"
        enc=$(python encrypt.py "$data")
        echo $enc | nc -4u -w1 127.0.0.1 6666
done
```

Listing 5: Send with replay protection - Bash script

```
while true
do
        response=$(nc -w 1 -vvul 0.0.0.0 6666 2>&1)
        decrypt=$(python decrypt.py $response)
        timestamp=$(date +%s)
        IFS=’:’ read -r -a array <<< "$decrypt"
        diff="$(($timestamp - ${array[0]}))"
        if [ "$diff" -le "1" ]; then
                echo ${array[1]}
                # Obey command ...
        fi
done
```

Listing 6: Receive with replay protection - Bash script

Bibliography

[1] J. Stamp. Unmanned Drones Have Been Around Since World War I. Accessed: 2016-02-22. [Online]. Available: http://www.smithsonianmag.com/arts-culture/unmanned-drones-have-been-around-since-world-war-i-16055939/?no-ist

[2] The Radioplane OQ-2 aerial target drone was the first quantitative UAV purchase for the United States. Accessed: 2016-02-22. [Online]. Available: http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=331

[3] (2015, apr) The V Weapons. Accessed: 2016-06-24. [Online]. Available: http://www.historylearningsite.co.uk/world-war-two/world-war-two-in-western-europe/the-v-revenge-weapons/the-v-weapons/

[4] PD-100 PRS. [Online]. Available: http://www.proxdynamics.com/products/pd-100-black-hornet-prs

[5] M. Mazur, A. Wiśniewski, and J. McMillan, "Clarity from above," 2016. [Online]. Available: http://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf

[6] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Uavs for smart cities: Opportunities and challenges," in *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on.* IEEE, 2014, pp. 267–273.

[7] J. Lejot, C. Delacourt, H. Piégay, T. Fournier, M.-L. Trémélo, and P. Allemand, "Very high spatial resolution imagery for channel bathymetry and topography from an unmanned mapping controlled platform," *Earth Surface Processes and Landforms*, vol. 32, no. 11, pp. 1705–1725, 2007. [Online]. Available: http://dx.doi.org/10.1002/esp.1595

[8] Ambulance drone. Accessed: 2016-02-23. [Online]. Available: http://www.alecmomont.com/projects/dronesforgood

[9] Dronewallah. (2015) Knowledge Base: What are RTF, BNF and ARF drone kits? Accessed: 2016-04-15. [Online]. Available: http://www.rcdronearena.com/2015/02/23/what-is-rtf-bnf-arf-drone-kit/

[10] Danish Transport Authority. (2015) Future regulation of civil drones. Accessed: 2016-02-29. [Online]. Available: https://www.trafikstyrelsen.dk/~/media/Dokumenter/05%20Luftfart/01%20Publikationer%20luftfart/Report%20on%20civil%20drones.ashx

[11] (2016, apr) Enkle og klare regler på droneområdet (only Danish). Accessed: 2016-06-24. [Online]. Available: http://www.trm.dk/da/nyheder/2016/enkle-og-klare-regler-paa-droneomraadet

[12] K. Andersen, "Høring over udkast til ny dronebekendtgørelse (only Danish)," 2016. [Online]. Available: http://prodstoragehoeringspo.blob.core.windows.net/700c13e0-3aac-40e6-807e-68d4d27d4367/Dronebekendtg%C3%B8relse%20h%C3%B8ringsbrev%200806.pdf

[13] UDKAST til: Bekendtgørelse om flyvning med droner i bymæssigt område (only Danish). [Online]. Available: http://prodstoragehoeringspo.blob.core.windows.net/700c13e0-3aac-40e6-807e-68d4d27d4367/Bekendtg%C3%B8relse%20om%20flyvning%20med%20droner%20i%20by_H%C3%98RINGSUDKAST.pdf

[14] Wi-Fi Alliance. (2015) Total Wi-Fi® device shipments to surpass ten billion this month. Accessed: 2016-02-29. [Online]. Available: http://www.wi-fi.org/news-events/newsroom/total-wi-fi-device-shipments-to-surpass-ten-billion-this-month

[15] J. M. Tjensvold. (2007) Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards. Accessed: 2016-03-

01. [Online]. Available: https://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf

[16] (2015, dec) Skier Marcel Hirscher escapes injury as drone smashes behind him during race. Accessed: 2016-06-24. [Online]. Available: https://www.theguardian.com/sport/2015/dec/23/champion-skier-marcel-hirscher-has-near-miss-as-drone-falls-out-of-sky

[17] (2011, dec) How Iran hacked super-secret CIA stealth drone. Accessed: 2016-06-15. [Online]. Available: https://www.rt.com/usa/iran-drone-hack-stealth-943/

[18] (2015, oct) UK police see spike in drone incidents. Accessed: 2016-06-24. [Online]. Available: https://www.theguardian.com/technology/2015/oct/11/drone-incidents-reported-to-uk-police-on-the-rise

[19] A. Shoufan, H. AlNoon, and J. Baek, *Information Systems Security and Privacy: First International Conference, ICISSP 2015, Angers, France, February 9-11, 2015, Revised Selected Papers.* Cham: Springer International Publishing, 2015, ch. Secure Communication in Civil Drones, pp. 177–195. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-27668-7_11

[20] D. Martins and H. Guyennet, “Wireless sensor network attacks and security mechanisms: A short survey,” in *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, Sept 2010, pp. 313–320.

[21] A list of wireless network attacks. Accessed: 2016-06-08. [Online]. Available: http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks

[22] E. Barker, M. Smid, and D. Branstad, “A Profile for U. S. Federal Cryptographic Key Management Systems,” *NIST Special Publication 800-152*, 2015. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-152

[23] Organización Internacional de Normalización, *DS/ISO/IEC 27005: Information technology-Security techniques-Information security risk management*, 2nd ed. DS, 2011.

[24] M. S. Lund, B. Solhaug, and K. Stlen, *Model-Driven Risk Analysis: The CORAS Approach*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[25] Netcat. [Online]. Available: http://netcat.sourceforge.net

[26] Wireshark. [Online]. Available: https://www.wireshark.org

[27] Tcpreplay. [Online]. Available: http://tcpreplay.synfin.net

[28] SYMA X5SW. [Online]. Available: http://www.symatoys.com/product/show/1927.html

[29] Hubsan X4. [Online]. Available: http://www.hubsan.com/productinfo_16.html

[30] PhracturedBlue. Hubsan X4 protocol analysis - RC Groups. Accessed: 2016-05-30. [Online]. Available: http://www.rcgroups.com/forums/showthread.php?t=1773853

[31] Aircrack-ng. [Online]. Available: http://www.aircrack-ng.org

[32] Parrot AR.Drone 2.0. [Online]. Available: http://www.parrot.com/usa/products/ardrone-2/

[33] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," *Homeland Security Journal*, vol. LAUR-03-6163, pp. 22–30, 2003, [Online]. Available: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-6163.

[34] L. Vaas. (2012, jul) Drone hijacked by hackers from Texas college with $1,000 spoofer. Accessed: 2016-06-15. [Online]. Available: https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/

[35] J. Cook. (2015, jan) This Hacker Figured How to Hijack One of the Most Popular Drones. Accessed: 2016-06-15. [Online]. Available: http://www.slate.com/blogs/business_insider/2015/01/27/hacking_drones_parrot_drones_can_now_be_hijacked_mid_air_through_malware.html

[36] L. Kelion. (2013, dec) Parrot drones 'vulnerable to flying hack attack'. Accessed: 2016-06-15. [Online]. Available: http://www.bbc.com/news/technology-25217378

[37] B. Benchoff. (2015, oct) Hijacking Quadcopters with a MAVLink Exploit. Accessed: 2016-06-15. [Online]. Available: http://hackaday.com/2015/10/15/hijacking-quadcopters-with-a-mavlink-exploit/

[38] R. Krishnan. (2016, feb) NASA HACKED! AnonSec tried to Crash $222 Million Drone into Pacific Ocean. Accessed: 2016-06-15. [Online]. Available: http://thehackernews.com/2016/02/nasa-hacked-drone.html

[39] J. Murdock. (2016, mar) Drone hack: Weak encryption leaves high-end UAVs wide open to remote hijacking. Accessed: 2016-06-15. [Online]. Available: http://www.ibtimes.co.uk/drone-hack-weak-encryption-leaves-high-end-uavs-wide-open-remote-hijacking-1547356

[40] P. Sneiderman. (2016, jun) Johns Hopkins scientists show how easy it is to hack a drone and crash it. Accessed: 2016-06-15. [Online]. Available: http://hub.jhu.edu/2016/06/08/hacking-drones-security-flaws

[41] (2016, jun) British drone-freezing ray gets US airports trial. Accessed: 2016-06-01. [Online]. Available: http://www.bbc.com/news/technology-36425879