Unmanned Aerial Vehicles: Vulnerability to Cyber Attacks

Susheela Dahiya and Manik Garg

Abstract With the increase of technological capabilities of automated systems, the use of unmanned aerial vehicles (UAVs) has also increased in many military and civilian applications. UAVs today play an important role in many other areas like wildlife surveys, weather monitoring, monitoring natural disasters affects etc. It is also expected that UAVs will be a major part of future smart cities. The amount and type of information present with UAVs makes it an extremely interesting target for cyber-attacks. However, the cybersecurity aspect of UAVs has not been fully considered while building UAVs. As a result, UAVs are more vulnerable to cyber-attacks. Potential security vulnerability may exist in the modules, which are responsible for their proper working or may exist during communication between UAVs and control station. Out of these two, communication security is critically important for the success of UAVs as they often carry sensitive information that adversaries might try to get hold of. Wi-Fi attacks such as Eavesdropping, Information Injection, Denial-of-Service, and Distributed DoS are the possible security threats to UAV communications. Recently, GPS spoofing attack, session hijacking, and compromised surveillance are also reported. The goal of this paper is to provide the different levels of vulnerabilities along with the prevention measures required at each level, some major attacks that can be performed on a UAV along with their cause, impact and the precautions required to avoid that attack. It has been observed that the most easily attackable vulnerability on the UAV system is flooding the UAV using the radio communication and the most harmful vulnerability is acquiring complete control through Man-in-the-Middle attack.

Keywords UAV · Vulnerability · Threat · Security · Network attacks

1 Introduction

Unmanned Ariel Vehicle is a drone without any direct human control. It is helpful in various tasks such as guided surveillance [1], weather monitoring [2], unmanned

S. Dahiya (✉) · M. Garg
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India

K. Jain et al. (eds.), *Proceedings of UASG 2019*, Lecture Notes in Civil Engineering 51,
https://doi.org/10.1007/978-3-030-37393-1_18

attacks, covert intrusions, enemy reconnaissance, aircraft maintenance and repair operations, military training [3], cargo transportation, disaster relief [4], rescue operations [5], search operations, tracking operations [6] etc. It is operated and guided from a remote location also known as the control center. A control center is typically a place with a transmitter and a controller (human) that gives commands to the UAV with the help of remote connection sending instructions through a communication channel using radio waves. Apart from radio waves, GPRS & EDGE technologies are also used for communication between the UAV transceiver and the control center transceiver.

The surveillance video data collected by UAVs is confidential and time sensitive that need to be shared on immediate basis. Any unauthorized access or delay in data transmission can result in mission failure [7]. Since there is a remote communication between the UAV transceiver and the control center transceiver through the atmospheric medium, it is susceptible to a huge number of cyber-attacks. The technologies used for communication with UAV such as radio, GPRS & EDGE works by means of packets contacting a small block of data. A packet traveling over a network needs to be secured from various threats that can in any way change the packet or result in sharing the data with unauthorized users.

The contents of this paper organized in eight sections. The first section aims at providing an introduction about the role of a UAV and the importance of its security. The second section deals with the various vulnerabilities associated with the UAV. Categorization of Attacks are discussed in the third section. The attacks that can be performed on a UAV are explained in the fourth section. The fifth section deals with the recent attacks on UAVs, their cause and cure. Prevention measures required on different levels of UAVs are explained in sixth section. The seventh section suggests some measure to protect UAVs against these attacks. Finally, section eight concludes the paper.

2 Vulnerabilities

In UAVs, the vulnerabilities can be at any of the following three levels: Transceiver Level, Control Center Level and Communication Channel Level. Out of these three levels, the threats at transceiver level and communication level are from outsiders but in case of control center, an insider can also be a threat [8]. The following subsections gives a brief overview of the vulnerabilities associated with each level.

2.1 Transceiver Level

The UAVs major component is its CPU along with its transceiver. The transceiver fulfills the function of transmitting and receiving packets to and from the control center through the communication channel. Since UAVs are also used for military

surveillance thus, the traffic that is incoming as well as outgoing can be highly crucial and sensitive. The UAV should verify the incoming traffic for authenticity and integrity but if it fails to do so, there can be a flow of some illegitimate packets that can contain some wrong instructions for the UAV. The main vulnerability at this level is non-validation of the packets received. If any unwanted command is issued to the UAV and it acts upon it then, it may lead to unauthorized and unaccounted attacks. In addition to that, the whole surveillance system can be taken down.

2.2 Control Center Level

The control center is the brain of the UAV since all the control lies within the control center. The main threat to any asset is always the insiders i.e. any user who has rogue intentions. Other vulnerability lies on the network providing access to the control center where various attacks can be performed. If the control center is compromised, then the surveillance system can be hijacked. The access to control center network may contain vulnerabilities such as SQL injection which may lead to access to the network from a person who can be a threat. Also, if there are no Backup servers in the control center or load balancers are not set up then the whole control mechanism service can be taken down by flooding requests that will cause incomplete TCP Handshake [9].

2.3 Communication Channel Level

All the control instructions for the UAV travels through this medium. The data traveling needs to be encrypted else if intercepted can cause major harm to the UAV and the organization owning it. Apart from interception, the communication channel can be a medium to perform various types of active attacks. Various vulnerabilities from the OWASP top 10 list can be found over the communication medium. Since communication is mainly done using radio waves or GPRS/EDGE, the connection is very insecure and can be compromised easily. Also, while establishing a connection, using less secured protocols can also lead to compromised security [10].

3 Types of Attacks

The attacks that can be performed on a UAV depends on the vulnerability that the attacker is targeting. Since, there are three major targets in the whole UAV system i.e. UAV transceiver, communication channel, and the control center, there can be single or multiple vulnerabilities that can be targeted at a particular instance of time. The attacks that can be performed can be categorized into the following two categories.

3.1 Active Attacks

This type of attacks comes under the penetration testing part of the Ethical Hacking system. In such attacks, the main aim is to disrupt the services or perform a breach without caring about the interruption in the original transmission. These attacks are done in the real-time i.e. at $t = 0$ and are completed as soon as the required data or aim is achieved.

3.2 Passive Attacks

This type of attacks usually involves network monitoring, port listening or packet sniffing. In such attacks, the attacker usually sits on the network silently without the knowledge of the user and thus there is no interruption in the original transmission. The attacker captures the needed packets and afterward performs analysis on them to attain the required information such as secret keys or digital certificate algorithms.

4 Attacks and Their Risk Factors

Man-in-the-Middle attack, Denial of Service attack and Command Injection attack are the three main attacks that can performed on a UAV [11]. Each attack will cause a different kind of loss. That loss can be either a minor financial loss or a major industry collapse or a security threat. The cause and risk factor associated with the attacks that can be performed on a UAV system are explained in the following subsection.

4.1 Man-in-the-Middle Attack

This attack can be of both types either passive or active. In this attack, the attacker intercepts the traffic between the legitimate sender and the receiver and performs either reconnaissance or data tampering. This attack may lead to a data breach or a major loss in data integrity. Data Integrity is the most important part of the CIA triad and it needs to be preserved. This attack is possible by capturing the sharing of keys at the time of connection establishment. Other possible ways to attain this attack are IP spoofing, ARP poisoning, DNS poisoning, ARP spoofing, DNS spoofing, SSL hijacking, HTTPS spoofing and many more. The following image depicts a simple Man-in-the-Middle attack and demonstrates how the traffic is redirected from sender to attacker and then to the receiver [12] (Figs. 1 and 2).

The main concept on which this attack works is multiple TCP handshake establishments [13].

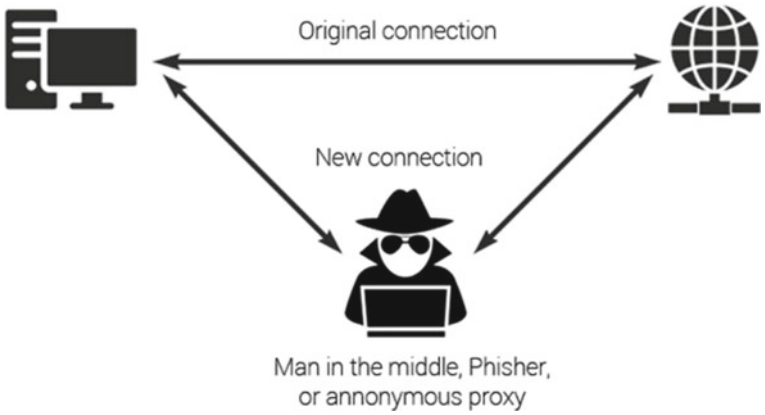

Fig. 1 Man-in-the-Middle attack [12]

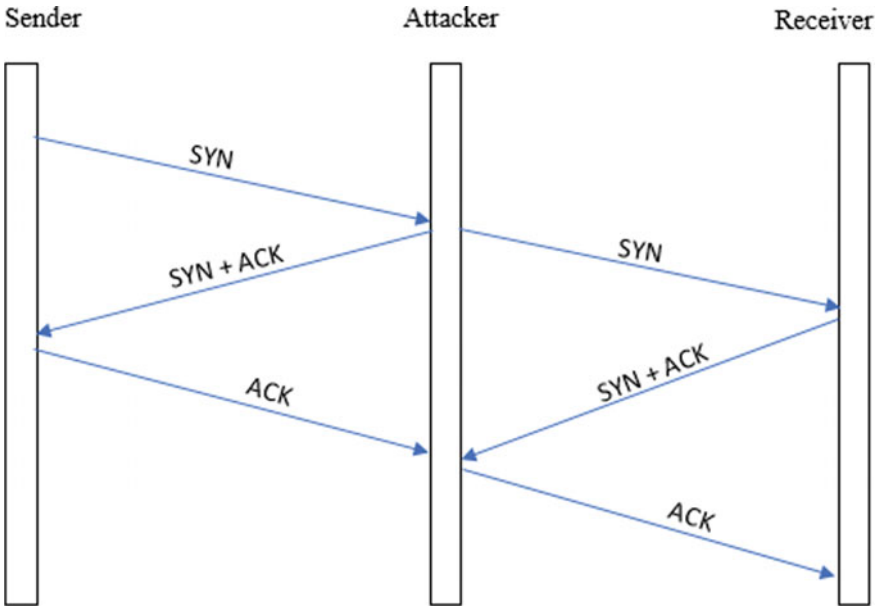

Fig. 2 Multiple TCP handshake in MITM attack

In the UAV communication channel if a MITM attack is performed it may lead to compromised surveillance, session hijacking, unauthorized activities, unauthorized attacks (in case of military UAVs), wrong data, change of projectile of UAV and much more.

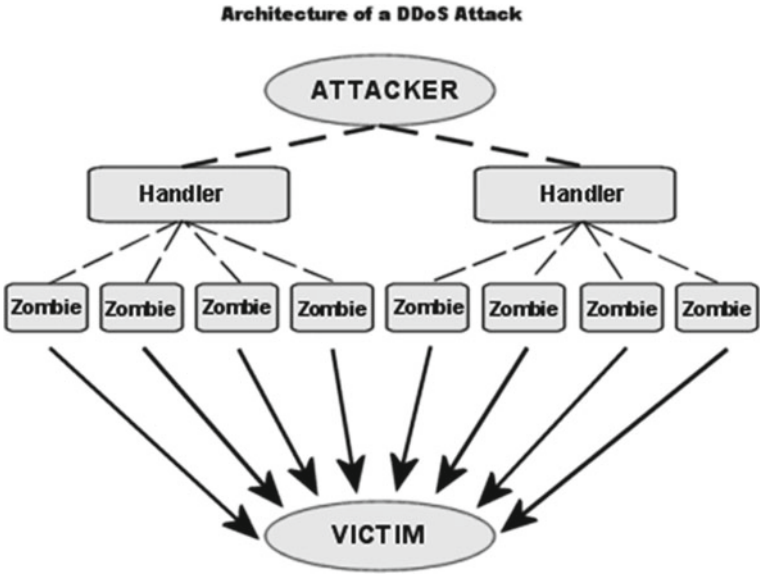

Fig. 3 Representation of distributed denial of service attack [14]

4.2 Denial of Service Attack

This is a type of active attack. In this attack, the attacker floods a huge number of packets to the target. These packets serve as multiple requests to the target and when the target is unable to serve these many requests, it crashes. These packets can be either TCP SYN packets or normal ping packets. An upgraded version of this attack also exists known as the Distributed Denial of Service attack (DDoS). In this attack instead of using a single source to flood packets, the attacker uses multiple sources controlled by him to flood packets. These sources are known as zombies. The complete network of zombies used to perform the attack is known as Zombie Net. The Fig. 3 explains the DDoS Attack.

As a result of a DDoS attacks the server will not be able to serve the requests of legitimate users. Thus, if a DDoS attack has been performed on the UAV transceiver or the control center using the UAV communication channel it may lead to loss of communication between the UAV and the control center. As a result, the UAV can be lost and some packets containing sensitive information may also be destroyed [14].

4.3 Command Injection Attack

This is also a type of active attack. In this attack, a piece of code is injected in the HTML based application. This injected code is malicious in nature and runs a script

that can help in providing unauthorized access and data tampering. If a command injection vulnerability exists in the UAV control center or the UAV Drone, then the whole system can be compromised and taken in control by some external entity.

4.4 Privilege Escalation Attack

This is also a type of active attack. In this attack, the user performs operations that he/she is not authorized to perform by acquiring privileges of a higher authority. This happens due to weak access control systems or default passwords usage in admin systems.

4.5 IP Spoofing Attack

This is also a type of active attack. In this attack, the source of the requests is changed to a legitimate source by means of IP Spoofing. It refers to disguising the original IP address with some other fake IP address. Thus, if a firewall is configured in the UAV system to allow access from certain fixed IPs, this attack can be used to gain access.

5 Cyber Attacks on UAVs

UAV's could be hacked and turned into weapons. Thus, monitoring of UAVs is a big issue that needs to be addressed. Following are some attacks performed by using UAVs

I. In 2009, a terrorist group was found to have captured an unencrypted UAV video feed using SkyGrabber (a software for capturing free satellite videos) [15].
II. In 2011, Iran Cyber unit was able to acquire control over US army drones and received various sensitive information from these drones. This was also possible due to the weak security measures implemented on the drones [16].
III. In 2017, a Chinese drone was hacked. A Cyber Security Response Team from US did this and this team was able to find many vulnerabilities in this drone [17].
IV. On August 5, 2018, two drones were used by some terrorist organizations to carry out an attack on the President of Venezuela. These drones were packed with explosives. The main area of concern lies at how these drones were able to reach that near to the President [18].

6 Prevention of Vulnerabilities in UAV

There are various ways to prevent the UAV system from the attacks and threats that can exploit the vulnerabilities that exist in different modules of the UAV system. The prevention measures required at each level are explained in the following sub sections.

6.1 Communication Channel Level

The traffic that travels on the network, typically the sensitive information or the UAV control commands should be sent in an encrypted manner using some asymmetric cryptographic algorithms. Also, to provide safe integrity these packets should be associated with a hash value that can be checked at a later stage. Another measure that can be applied is checksum that also serves as a check to integrity. Also, while using wireless communication some secure protocols such as HTTPS, SSL, TLS, etc. should be used so as to serve requests in a better way using secure session management techniques.

6.2 Transceiver Level

Since this module is susceptible to various attacks such as DDoS & Session Hijacking so there should be some security and intelligent rules that should be implemented. The most secure way is to implement a firewall at the UAV that can filter the packets that are received. Rules should be configured in the firewall so that it only allows traffic from only one IP address i.e. from the control center server. This IP whitelisting will prevent DoS attacks as all other packets will be dropped immediately and also no malicious code will be able to reach the UAV. Since there are still chances of IP spoofing in this implementation thus an IDPS (Intrusion Detection & Prevention System) should be implemented to prevent any further intrusion.

6.3 Control Center Level

Since control center also has various vulnerabilities thus the first thing that shall be acted upon is access management. The access to the control center should be well maintained as it comes under a high-security zone. Measures such as Input Validation, Access log management, Concept of Least privilege should be implemented. In addition, since there is a huge possibility of DoS attack on the control center server, firewall and load balancers should be implemented with IP whitelisting rules. Also,

the internet and the intranet should be bridged by a secure firewall or IDPS. To prevent data breaches or data destruction attacks, backup servers should be kept and updated at fixed intervals so that no crucial information is lost.

7 Results

It has been found that there are many vulnerabilities that exist on the UAV system like SQL injections, DoS attack, Man-in-the-Middle attack, Elevated Privileges and IP spoofing. Among these vulnerabilities, few are of high risk and few of low risk. The precautions required to avoid the vulnerabilities are as follows:

i. SQL/Command Injection vulnerability can be fixed by using input validation and strict type checking using sanitization of data received.
ii. To avoid DoS attack, the server and the UAV should be both able to handle huge number of packet flooding. This can be fixed using load balancers or IP whitelisting rules. Also, an IDPS or firewall should be setup that can detect and prevent from a possible DoS attack.
iii. Man-in-the-Middle vulnerability can be prevented by using secure transmission protocols, integrity checks, encrypted traffic and usage of VPNs (Virtual Private Networks).
iv. To prevent Elevated Privileges vulnerability strict access control mechanisms and access rights systems should be implemented. The network administrator should also regularly change default passwords and delete unused accounts.
v. IP spoofing vulnerability can be prevented by performing IP subnetting and masking. Also, there should be confidentiality involved while sharing these IP addresses as they are a crucial asset in this communication system.

8 Conclusion

The most easily attackable vulnerability on the UAV system is flooding the UAV using the radio communication. The most harmful vulnerability on the other hand is acquiring complete control through Man-in-the-Middle attack. These things need to be carefully addressed and worked upon. The amount of security measures to be deployed on a UAV depends upon the type of task it is being used for. Some crucial UAVs that are used for military or weather surveillance are more susceptible to attacks rather than normal event coverage drones. Also, the UAVs performing delivery operations can be targeted by some thieves. Specially the military drones that also have the capabilities to attack can be most targeted ones and need to have best security measures to be implemented.

Along with cybersecurity threats associated with UAV, we should always keep into consideration the other threats such as physical security threats, weather related

issues, accidental collisions or intentional collisions and also most importantly drone capturing. Although UAVs bring a lot of automation and ease at many tasks, they also bring along a huge number of threats that needs to be addressed and worked upon based on their risk assessment depending on their impact and likelihood determination.

References

1. Kim A, Wampler B, Goppert J, Hwang I, Aldridge H (2012) Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In: AIAA Infotech@Aerospace. https://doi.org/10.2514/6.2012-2438
2. Gupta SG, Ghonge MM, Jawandhiya PM (2013) Review of unmanned aircraft system (UAS). Int J Adv Res Comput Eng Technol (IJARCET) 2(4)
3. Udeanu G, Dobrescu A, Oltean M (2016) Unmanned aerial vehicle in military operations. Sci Res Educ Air Force 18(1):199–206. https://doi.org/10.19062/2247-3173.2016.18.1.26
4. Debusk W (2010) Unmanned aerial vehicle systems for disaster relief: Tornado Alley. In: AIAA Infotech@Aerospace 2010. https://doi.org/10.2514/6.2010-3506
5. Waharte S, Trigoni N (2010) Supporting search and rescue operations with UAVs. In: 2010 international conference on emerging security technologies. https://doi.org/10.1109/est.2010.31
6. Javaid AY, Sun W, Devabhaktuni VK, Alam M (2012) Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In: 2012 IEEE conference on technologies for homeland security (HST), Waltham, MA, pp 585–590. https://doi.org/10.1109/ths.2012.6459914
7. Benkraouda H, Barka E, Shuaib K (2018) Cyber-attacks on the data communication of drones monitoring critical infrastructure. Comput Sci Inf Technol (CS & IT) 8:83–93. https://doi.org/10.5121/csit.2018.81708
8. Brauch H (2019) Security threats, challenges, vulnerability and risks international security, peace, development and environment, vol I. In: Security threats, challenges, vulnerability and risks
9. Aslanishvili I, Khvedelidze T (2015) Simple model for transmission control protocol (TCP). Int J Inf Models Anal 4(1)
10. Rafique S, Humayun M, Hamid B, Abbas A, Akhtar M, Iqbal K (2015) Web application security vulnerabilities detection approaches: A systematic mapping study. In: 2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD), Takamatsu, 2015, pp 1–6. https://doi.org/10.1109/snpd.2015.7176244
11. Gudla C, Rana MS, Sung AH (2018) Defense techniques against cyber attacks on unmanned aerial vehicles. In: International conference on embedded systems, cyber-physical systems, and applications (ESCS'18), pp 110–116
12. Secure BOX Page. https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/. Last accessed 2019/02/24
13. https://www.reuters.com/article/us-venezuela-politics-drones/apparent-attack-in-ve-nezuela-highlights-risk-of-drone-strikes-idUSKBN1KQ0MG. Last accessed 2019/03/01
14. DoS Attacks. https://www.thewindowsclub.com/ddos-distributed-denial-service-attacks. Last accessed 2019/02/24
15. He D, Chan S, Guizani M (2017) Communication security of unmanned aerial vehicles. IEEE Wirel Commun 24(4):134–139
16. https://doi.org/10.1109/mwc.2016.1600073wc

17. https://sputniknews.com/middleeast/201902221072659058-iran-hack-us-drones/. Last accessed 2019/03/02
18. https://www.forbes.com/sites/thomasbrewster/2017/04/25/vulnerable-quadcopter-d-rone-hacked-by-ut-dallas-cyber-researchers/#1b4103871037. Last accessed 2019/03/03