Vulnerability and Threat Analysis of UAVs

Burak Tufekci[1] and Cihan Tunc[2]

[1,2]*Department of Computer Science & Engineering, The University of North Texas, TX, US*
[1]Burak.Tufekci@unt.edu, [2]Cihan.Tunc@unt.edu

2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA) | 978-1-6654-0969-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/AICCSA53542.2021.9686826

***Keywords*—UAV, Cybersecurity, Threat Modeling**

I. Extended Abstract

The usage and application areas of Unmanned Aerial Vehicles (UAVs) are increasing such as military services, live streaming events, aerial photography, agriculture, firefighting, product delivery, asset inspections, and so on owing to bringing along the many benefits with it. According to Federal Aviation Administration (FAA), 865,660 drones (or UAVs) are registered and of these, 340,247 are commercial drones, 521,819 are recreational drones, 3,594 are paper registrations [1].

Due to the widespread utilization of UAVs, taking cybersecurity measures of UAVs has become inevitable. Sandra et. al have proposed the exploitation of GPS vulnerability for the commercial company 3D Robotics [2]. Restituyo et al. have presented the exploitation of jamming, GPS spoofing, packet sniffing, and video replay [3]. Besides, Todd et al. have succeeded to land a UAV without its operator's knowledge by spoofing UAVs' GPS system [4].

There are many vulnerabilities and possible attacks in the literature. Failure to take the necessary precautions against those vulnerabilities may result in damage of assets or complete loss. Therefore, this paper focuses on analyzing cyberthreats against UAVs and applying threat modeling.

UAVs can have flight controllers, communication systems, actuators, gyros, cameras, and different sensor types based on application as shown in the Fig 1. UAVs can communicate with either their allies or the Ground Control Station (GCS). If there is a communication link between two or more UAVs, it is called Flying Ad-Hoc Network (FANET). The existing Ad-Hoc security solutions can be insufficient for FANET because FANET's features are completely different from existing Ad-Hoc Networks such as Mobile Ad-Hoc Network (MANET) and Vehicle Ad-Hoc Network (VANET).

Since UAVs include many physical and software-based components, considering the fact that each component would increase the attack vector, we need to examine the components carefully and apply threat modeling. In what follows, we summarize some main UAV components.

Sensors: UAVs sense the environment or set their position by using of sensors. Some commonly used sensors in UAVs are,

- **Position Sensors**: detect the presence of the objects
- **Gyroscope Sensors**: detect angular movement of the objects
- **Velocity Sensors**: detect the speed of the objects
- **Infrared Sensors**: detect infrared radiations of the objects
- **Temperature Sensors**: detect the temperature of the environment
- **Proximity Sensors**: detect the position of the objects by emitting EM wave

Inertial Measurement Units (IMUs): UAVs need to stabilize their movement in the air. This process requires IMUs, which take an action according to rapid changes in the air. Some preferred IMU types in UAVs are,

- **Silicon/Quartz MEMS**: Higher vibration, noise sensitivity (ideal for commercial)
- **Fiber-Optic/Ring-Laser Gyro**: Provides high performance on angle random walk and thermal stability (ideal for military)

Actuators: are mechanism that perform given operation. Some common used actuator type in the UAVs are,

- **Servo Linear Actuators**: They provide a linear action (i.e., movement) such as rudder to change the direction of the planes.
- **Servo Rotary Actuators**: They are responsible for angular movements (for opening and closing landing gear).
- **Flight Control Actuator**: controls flight control surfaces on UAVs (the ailerons, tailerons, rudders and flaps.)

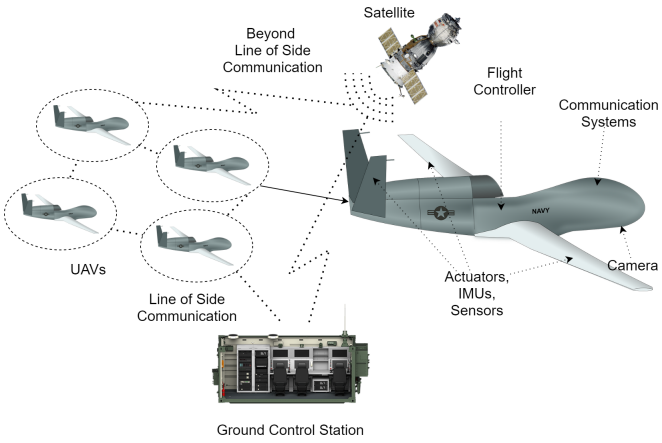

Fig. 1. FANET and UAV architecture

There are also communication systems, flight controllers, and cameras on UAVs. For threat analysis, we used STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege) and DREAD (Dam-

TABLE I
POSSIBLE THREATS AND THEIR IMPACTS

Domain	Threat	STRIDE	DREAD	Consequences	Detection	Mitigation
Physical	Insider Attacks	Info Disc.	(10+7+2+1+10)/5	Possible Info Leaking	Logging and Notifier	Give Least Privileges
Physical	Stealing and Vandalism	DoS	(10+4+5+1+10)/5	Possible Harm to UAV	Logging and Notifier	Fail/Safe protocol
Physical	(Sensor) Corruption	Spoofing	(10+2+2+1+10)/5	Possible Harm to UAV	IDS	ML-Based Monitoring
Physical	(Actuator) Corruption	Spoofing	(10+2+2+1+10)/5	Possible Harm to UAV	IDS	ML-Based Monitoring
Network	Packet Modificaton	Tampering	(5+7+2+1+10)/5	Disrupt UAV Functions	Verify MAC	Data Encryption
Network	Code Injection	EoP	(10+7+2+1+10)/5	Disrupt UAV Functions	Firewall or IDS	Strong Sec. Pol.
Network	Packet Sniffing	Info Disc.	(2+9+8+1+10)/5	Possible Info Leaking	Anti Sniff Tools	Data Encryption

age, Reproducibility. Exploitability, Affected Users, Discoverability) techniques.

In Table I, we demonstrate threat modeling for UAVs and explain for which domains they can be related to. We explain the relative threats, apply STRIDE, rank them using DREAD, explain possible consequences, and show detection and mitigation techniques.

There is always a potential risk for information leakage from inside. Hence, we need to apply the least privilege principle here to decrease information disclosure. The effect of the information leakage on the system is considered a high potential risk. The Damage is high (10), the Code Path is easily understood (7), Exploitable is hard (2), Affected Users (1), and Discoverability is always assumed 10. When we sum them up and divide them into 5, we reach 6 and this ends up with 6 DREAD score.

There is always a possibility that the drone is compromised and the ground station could have no information about it. We can simply apply Fail/Safe protocol here, however, the risk of damage is considered as high here and thus, we have graded it as 6.

The sensor and actuator spoofing is always hard to detect. However, using ML-Based monitoring can decrease that type of attack. The IDS can be a solution for detection. They are graded as 5.

Since Message Authentication Code (MAC) provides both message integrity and confidentiality, if our communication packets are encrypted with proper MAC, we ensure that our data packets are not changed or leaked. Usually, the UAVs prefer to use SSL/TLS communication protocol and we are sure that the communication channel is trusted. Sometimes, UAVs may choose different protocols, such as Micro Air Vehicle Link (MAVLink), to communicate with each other and the researchers have found that MAVLink protocol is insecure [5]. Thus, we have graded it as 5.

Although many firewalls and Intrusion Detection Systems (IDS) offer prevention against Code Injection, some malware code uses encode mechanisms to bypass firewalls or IDS. Therefore, we need to provide strong security policies to ensure all data and commands are meaningful. If the security policies aren't configured properly, the potential risk of the system would be higher. Hence, we have graded it as 6.

Even though there are some detection tools against packet sniffing, it is hard to detect sniffers because they are always passive in the communication channel. As a solution we make sure that the communication channels are encrypted and the keys are not re-used and we change them frequently. Therefore, we have graded it as 6.

REFERENCES

[1] T. Report, "UAS by the Numbers," Oct. 26, 2021. [Online]. Available: https://www.faa.gov/uas/resources/by_the_numbers/

[2] S. P. Arteaga, L. A. M. Hernández, G. S. Pérez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo," *IEEE Access*, vol. 7, pp. 51 782–51 789, 2019.

[3] R. Restituyo and T. Hayajneh, "Vulnerabilities and Attacks Analysis for Military and Commercial IoT Drones," in *IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 2018, pp. 26–32.

[4] T. E. Humphreys, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS," 2012.

[5] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," *IEEE Access*, vol. 6, pp. 43 203–43 212, 2018.

Burak TUFEKCI was born in Istanbul, Turkey. He received the BS degree in Electrical and Electronics Engineering from the Dokuz Eylul University, Izmir, Turkey, in 2018, and the MS degree in Computer Science from Ozyegin University, Istanbul, Turkey, in 2020. He has worked as Computer Hardware and Software Engineer in Baykar Defense Inc. between March 2021 and September 2021. Since September 2021, he has been pursuing a doctoral degree in the Computer Science and Engineering department at the University of North Texas. His current research interests include Cybersecurity, IoT, and UAVs.

Cihan TUNC was born in Istanbul, Turkey. He received the BS degree in Electrical and Electronics Engineering from the Bahcesehir University, Istanbul, Turkey, in 2008, and the MS degree in Electrical and Computer Engineering from Northeastern University, Boston, MA, in 2010. He received the Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, Tucson, AZ, in 2015. He has worked as Guest Researcher in the National Institute of Standards and Technology (NIST) between September 2016 and January 2020. Since January 2020, he has been working as an Assistant Professor in the Computer Science and Engineering department at the University of North Texas. His current research interests include Cybersecurity, Cyber-resiliency, Intrusion detection/prevention, Cyber-threat analysis in social media, Autonomic computing, Cloud computing, and IoT.