Anita Chidera Duanne Eluwa

20th February 2022

EG 6335 – Wireless Security

Glenn Howard – Academic Paper Review

Academic Paper Review: A Survey on Security and Privacy Issues of Unmanned Aerial Vehicles (UAVs)

INTRODUCTION

Unmanned Aerial Vehicles (UAV) sometimes known as drones is an airborne system or an aircraft operated remotely by a human operator or autonomously by an onboard computer. They were originally developed for military purposes and has greatly evolved with time concerning wireless communication and technology. UAVs are a component of an Unmanned Aircraft System (UAS), and this includes adding a ground-based controller and a system of communications with the UAV. In the academic research paper "A Survey on Security and Privacy Issues of Unmanned Aerial Vehicles (UAVs)", the authors (Mekdad, et al., 2021) explained in-depth the vulnerabilities of UAVs, the existing threats that are jeopardizing the civilian application of UAVs and how the complexity of UAVs in software and hardware triggers potential security and privacy issues. Some of the vulnerabilities highlighted include sensor-level issues, hardware-level issues, software-level issues, communication-level issues, as well as some privacy issues that will be analysed during this review. Our focus will however be on the security issues associated with UAVs. Although the evolution of UAVs has provided a lot of advantages to us the users in this new generation, the security vulnerabilities are faced in almost every technology and as the technologies evolve, the stakes are higher. These issues highlighted are however unique to UAVs. Additionally, the authors provide possible countermeasures and mitigation techniques to protect UAVs from malicious activities. To summarize this paper, we will begin by discussing the benefits of UAVs, the vulnerabilities and security issues found in them.

OVERVIEW

Unmanned Aerial Vehicles are considered as a newly emerging type of "flying IoT" device. This paper provides some benefits such as on-time parcel delivery and hostage rescue. There are however a lot more pros that they offer. Such as giving media access to hard-to-reach places, surveillance to private companies, sporting events, public gatherings, and other venues. Drones can also gather valuable data during and after natural disasters to aid in security and recovery efforts. Consequently, we will now analyse the vulnerabilities highlighted by the author. Because of how sensor-driven UAVs are, an adversary can exploit this vulnerability by simulating a GPS signal to delude the operator. From the perspective of an attacker, exploiting the onboard sensors' real-time data may cause a malfunction in the UAV's system. This can also lead to GPS data jamming and spoofing, false sensor data injection, and sensory-channel attacks.

The authors referenced works and surveys by other authors to provide countermeasures to these attacks. (Roth, 2009) provided a countermeasure "physical isolation for acoustic sensory channels to shield the sound noise" to mitigate sensory-channel attacks. But first, what are sensory channel attacks? Every UAV uses sensory channels like infrared, acoustic and a lot more and these channels can serve as a vector for attacks. Now the countermeasure provided could help with this attack but the question here is, how feasible will this be? To ensure that this mitigation can be implemented successfully, a large number of sensory channels will need to be considered. Originally, GPS spoofing happens when someone uses a radio transmitter to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal. To mitigate the attacks on GPS data spoofing, the authors suggested the adoption of authenticated schemes for GPS signals. To authenticate GPS signals, some changes in the infrastructure of the satellite will be made and then again, how feasible is that? Another threat that was mentioned is the false sensor data injection. One of the countermeasures provided by the authors is the cross-verification of data by gathering sensor readings from an alternative set of sensors. The major issue with this countermeasure is that adopting the existing solutions to other types of onboard sensors is still unknown.

The second category of threats is hardware-level threats. Some of the vulnerabilities found in the hardware of UAVs are hijacking, supply chain attacks, hardware failures. Hijacking in UAVs occurs when an attacker uses malicious software to attack the drones either remotely or physically (because of the low latitude of the drones). (Pu & Li, 2020) proposed the countermeasure of securing the GCS (Ground Control Station) and UAVs from unauthorized access using authenticated encryption. Encryption is one of the most effective measures of confidentiality and I think this security measure will minimize the likelihood of the system getting compromised. Hardware failures are one the most common threats in any system and for the UAVs, this might lead to an adversary getting access to stored data and the possibility of modifying the data. The authors referred to a countermeasure proposed by (Arslan, Mehmood, & Elhadef, 2021) to adopt encryption techniques on the flying UAVs that will prevent the adversary from capturing the stored data in the case of hardware failures. While this is a good security measure, I don't think it's good enough. When dealing with stored data and modification of data, Integrity and Availability needs to be considered. Encryption solves the issue of unauthorized users getting access to the data. But what if the data is lost, is there a means of recovery? Is there a backup plan put in place to get the data back? These factors should be considered as well. Hashing should also be considered as one of the security measures to prevent the stored data from being altered. Supply chain attack occurs in UAVs when other components of the system like propellers and airframes are compromised. This usually happens in the supply chain process of the company. (Zachary, Lueg, & LeMay, 2008) recommended managing the supply chain's security during the manufacturing process. One issue with this recommendation is that the manufacturing process is usually done internally. This might also lead to an insider or internal attack from one of its manufacturers. Hence, this needs to be watched closely.

The third category of threat highlighted is the software-level threats. Some of the vulnerabilities mentioned by the authors that are associated with UAV's software includes operating system attacks, malicious software, and system ID spoofing. When an operating system of the UAV is attacked, it affects the UAV system and its payload. The payload comprises the data and header which are the packets that are carried by the UAV devices. The authors recommended adopting the authorization mechanisms for UAV system resources. While this might be a bit challenging, it is also possible to implement. Operating system attacks can also lead to malicious software in the system because of its vulnerability. One important way to prevent this software is using firewalls and implementing intrusion detection systems to identify when a threat is present. Another challenge with software vulnerability is the zero-day vulnerabilities. Zero-day vulnerabilities are threats that are unknown to either the manufacturers or developers of a system. Because of these invisible threats, I recommend that the system should be updated and patched frequently to eliminate existing threats that won't be detected by the manufacturers or developers.

The last category of threats mentioned by the authors is communication-level issues. Communication issues deal more with the physical, MAC and network layers of the UAV. (Hooper, et al., 2016) demonstrated three different attacks affecting commercial Wi-Fi-based UAVs. These attacks are Buffer overflow, DoS attack, and ARP cache poisoning attack. Their experimental results reveal massive security issues in UAV-2-GCS wireless communications and choosing the correct type of wireless communication technology will depend on the specification of the mission requirements (e.g., transmission range, operating frequency, category, etc.). Some of these attacks like DOS, Eavesdropping and Man-In-The-Middle attacks (MITM) can also be present in the network layer. These are just a few of the threats found but the threats mentioned above are the most common found in UAV systems. The UAVs use a lot of communication technology like Wi-Fi, Bluetooth, Worldwide Interoperability for Microwave Access (WiMAX), Cellular Technology (GPRS, EDGE, UMTS/WCDMA, UMTS/HSPA, LTE, LTE Advanced - 4G, 5G) and a lot more. These technologies have their category (e.g., WLAN, WPAN), frequencies and range and for each communication channel, security issues are present. Most of the countermeasures provided by the authors include encryption, IDS solutions and secure-based protocols. However, implementing these security measures might not be compatible for all. For example, the authors recommend using IDS solutions to prevent DOS attacks, but this can lead to an anomaly-based IDS and cause false positives and negatives. Also, implementing these measures will require high computations and will increase energy consumption.

The four categories of threats encompass all the possible vulnerabilities that could potentially be found in UAVs. The authors, Mekdad, et al., did a survey with 23 other similar works on UAV vulnerabilities and provided a detailed explanation of each threat found in each layer. The intensity and depth of this paper are highly appreciated. In the course of this review, other works referenced were not as detailed because some layers of the UAV system were not identified. The surveys were done either for just the threats found in the sensor level and communication level or the hardware level and software level of the UAV but not all categories were highlighted. This makes this paper more detailed and emphatic than other works referenced.

CONCLUSION

The rapid evolution and improved technology of Unmanned Aerial Vehicles (UAVs) also known as drones provide efficiency to civilians, military personnel, civilian airspace, the government and a whole lot more. However, the higher the complexity and technology of the system, the higher the security issues. Manufacturers and software/system developers always consider security as “after the fact”, but with the deployment of new technologies in the UAV, security should be highly considered. The authors have provided extensive and detailed research on the whole architecture of the system, components, categories and the security threats/vulnerabilities associated with the UAV system both internally and externally. Although, there are still some loopholes that need to be considered in the countermeasures provided to remediate these security issues. We have identified the core issues with UAVs most especially at the communication-level and this survey will serve as a valuable reference for researchers to learn more about the design and implementation of a secure UAV and collectively figure out best practices to employ effective countermeasures to better the wireless communications in the system.

REFERENCES

Mekdad, Y., Aris, A., Babun, L., Fergougui, A. E., Conti, M., Lazzeretti, R., & Uluagac, S. (2021). A Survey on Security and Privacy Issues of UAVs. *arXiv preprint arXiv:2109.14442*, 1-26.

Roth, G. (2009). Simulation of the Effects of Acoustic Noise on MEMS Gyroscopes.

Pu, C., & Li, Y. (2020). Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System. *In 2020 IEEE International Symposium on Local and Metropolitan Area Networks*, 1-6.

Arslan, S., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access 9*, 46927-46948.

Zachary, W., Lueg, J. E., & LeMay, S. A. (2008). Supply chain security: an overview and research agenda. *The International Journal of Logistics Management*, 254-281.

Hooper, M., Yifan, T., Runxuan, Z., Bin, C., Adrian, L. P., Lanier, W., . . . Wlajimir, A. (2016). Securing commercial WiFi-based UAVs from common security attacks. *In MILCOM 2016-2016 IEEE Military Communications Conference*, 1213-1218.