Internet service via UAV- User centric comprehensive attack surface analysis

Sreejesh Sidharthan[†]
Computer Science
Georgia State University
Atlanta Georgia USA
ssidharthan1@student.gsu.edu

Ashwin Ashok (Advisor)
Computer Science
Georgia State University
Atlanta Georgia USA
aashok@gsu.edu

Anu Bourgeois(Advisor)
Computer Science
Georgia State University
Atlanta Georgia USA
abourgeois@gsu.edu

ABSTRACT

Usage of Unmanned Aerial Vehicles (UAVs) in civil application domains such as real-time monitoring, wireless internet, remote sensing, delivery of foods, security, and surveillance, and industrial infrastructure inspection has grown rapidly in recent times. The proliferation of UAVs in commercial and civilian use has increased the importance of security in these applications. In this paper, we are exploring the security threats associated with a civilian UAV use case. We are addressing the use case of UAVs providing internet to users and exploring the attack surface of UAV internet scenarios specifically focused on user-level security. We list specific threats associated with UAV internet scenarios and compiles various attack vectors to present a comprehensive attack surface analysis. This research work has identified 4 attack cases for the initial study. 1) Malicious UAV trying to exploit a user through the service. 2) Adversary targeting the legitimate UAV and users connected to the service. 3) User is targeted through malicious entity or a program in the user's device, and 4) External entity or a hacker attacking the user through a UAV communication channel. We are exploring the attack surfaces of the UAV internet use case extending the 4 cases mentioned above.

KEYWORDS

UAV, Drone, Adversary, Attack surface analysis, Internet of Drone(IoD), Threat Vectors

1 Introduction

UAVs are used in many civilian applications because of their fast deployment and extended mobility. Real-time monitoring of road traffic and wireless connectivity are some of the most common use cases. Many studies are being conducted across the world to evaluate the effectiveness and feasibility of UAVs to deliver various services to people. There are experiments of providing internet coverage using UAVs across areas where commercial internet connectivity is not available. Most of these studies and experiments were focused on feasibility and not much emphasis has been given to security. There are many papers are published that focus on the security of public -Wifi. Research work by Maimon et al. [1] has studied the situational awareness of public Wi-Fi users and their self-protective behaviors. Similarly, interesting papers are published on the security of Drones. Yaacoub et al. [2] provide one example of the research work on drone security focusing on the drone technical stack. In their paper, Yaacoub et al. [2]analyze the exploitation of a drone's vulnerabilities within communication links, as well as smart devices and hardware, including smartphones and tablets. Other research papers address drone vulnerabilities and utilizing these vendor vulnerabilities to defend users by making counter tools [3] [4]. Most of the studies are focused on attacking the drone using drone stack vulnerabilities or suggesting counter-drone techniques to defend. Moreover, most of the research considers an attacker-centric approach to find a solution to drone security. M. Yahuza et.al [5] have done a study on security and privacy issues of the Internet of Drones [IoD]. In their paper, M. Yahuza et.al focuses on classifying security and privacy issues of various drone categories and emphasis given to secured IoD architecture. Though this research gives an understanding of the security concerns in IoD networks, however, there are potential gaps in understanding the threats beyond the drone networks.

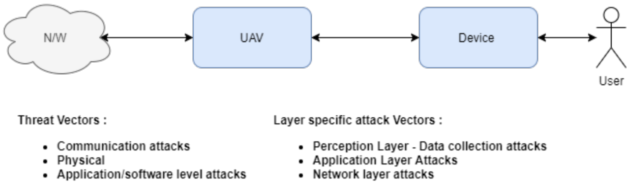
N/W
UAV
Device
User
Threat Vectors :
Communication attacks
Physical
Application/software level attacks
Layer specific attack Vectors :
Perception Layer - Data collection attacks
Application Layer Attacks
Network layer attacks

Figure 1: Current UAV-Service threat classification

Figure 1 captures the high-level summary of the current threats to a UAV service scenario where UAV is targeted. Broadly, we can classify threat vectors into 1)Communication level attacks, 2) Physical attacks and 3) Application or software level attacks. From a layer perspective, we can classify them into 1) Data collection layer attacks, 2) Application layer attacks, 3) Network layer attacks. From an extensive literature survey, we can say that we have not seen much information on how a user will get affected by the

S3 '21, October 29, 2021, New Orleans, LA, USA

ACM ISBN 978-1-4503-8704-0/21/10…$15.00
https://doi.org/10.1145/3477087.3478379

various classes of threat vectors listed above. The users, devices, communication channel, network, and service offered by the drones are the key components in the UAV service model. The more dynamic and diversified components are users and devices. Hence, it is more critical to understand the threat space from a user perspective. There are many unanswered questions when it comes to protecting the users and devices in the UAV network. We are exploring a comprehensive attack surface analysis of UAV internet service based on a user-centric approach. From a detailed literature survey conducted on the UAV civilian use case and security, we found that there are gaps in the current research considering the user-centric approach

2 Research Challenges

We are focusing on the user-centric-attack surface analysis of the internet-service-providing UAV to understand the security challenges to the user. Table 1 will give us a picture of how to model UAV-specific attack vectors, However, we do not have much information on how these attack vectors will play out in the specific use-case. There are limited resources to understand how a civilian UAV service can be targeted to attack users, data, and devices. The challenge here is to model user behavior and UAV service-specific vectors.

Layers	Common attacks	
Perception/Data collection layer	Tampering and Malicious code Injection	
Network Layer	Routing attacks DOS,DDOS attacks Network Injections and Sniffing	Remote code execution Malicious Firmware update Jamming
Application Layer	Data leakage -Privacy Code Vulnerabilities Application Layer DOS Misconfigurations	Sniffing attacks Reverse Engineering Power Exploitation

Table 1: UAV- layer-specific attack vectors

3 Proposed Research exploration

Our objective is to get a clear understanding of security challenges for the users and devices on the internet-providing- UAV scenario. As an initial step, we are intending to do an attack surface exploration on this use case and to extend if applicable in other similar scenarios. The following assumptions are taken here to address the user-centric model. 1) UAVs are providing legitimate internet connection . 2) Users are connecting to UAVs without prior registration process. Research focus is mainly to answer following questions or problems. 1) Are users or their devices secure enough to utilize the UAV -internet service? 2) What are the threat vectors in UAV-internet service specific to the users? We have identified 4 attack cases to initiate research. 1) Malicious UAV trying to exploit a user through the service – Here we are considering a rogue UAV attacking the user. 2) Adversary targeting the legitimate UAV and users connected to the service- Adversary targeting both users and UAV. 3) User is targeted through malicious entity or a program in the user's device – Users are attacked through their own devices. 4) External entity or a hacker attacking the user through a UAV communication channel – Here, the adversary's target is the communication channel between the UAV and user. We choose these 4 attack scenarios from a preliminary threat analysis on the service model. In all four cases users are the prime targets. The proposed model for Attack surface analysis is explained in Table 2.

Attack Scenarios	Methods(Not Limited)	Assets (Not Limited)
Malicious UAV to exploit a user through the service	Diversion of application logic, Malware Injection, Vulnerability Exploitation, and Remote attacks	PII, Confidential data, application info, network details, Location, file, device configuration, Connected device or network information
Adversary targeting the legitimate UAV and users.	Vulnerability Exploitation -Network or protocol Remote attacks Jamming, DOS, DDOS	PII, Confidential data, application info, network details, Location, file, device configuration, Connected devices, and network information.
Malicious program or code in user's device or network	Remote attacks Malware	PII, Confidential data, application info, network details, Location, file, device configuration, Connected devices, and network information
Adversary targeting the communication Channel	Jamming, DOS, DDOS Interception	Confidential data, Any Information passing through the channel

Table 2: Attack surface analysis model

The first attack scenario explained above will use the attack modes such as diversion of application logic, Malware Injection, vulnerability exploitation, and remote attacks. Targeted assets for the first case are PII, Confidential data, application, and device configurations, and network information. The second case mentioned above will use attack methods such as network and protocol vulnerability exploitation and remote attacks. In the third case malware and remote attack, methods will be employed. Targeted assets will be the same in the second and third scenarios. The fourth attack scenario will employ methods such as interception and jamming and the data passing through communication channels will be the prime target. We are considering exploring further on user's behavior to various attack methods mentioned above to construct a comprehensive attack surface analysis.

REFERENCES

[1] Maimon, David, C. Jordan Howell, Scott Jacques, and Robert Perkins. 2020. Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors. CrimRxiv, October. DOI: https://doi.org/10.21428/cb6ab371.b687013c.

[2] Jean-Paul Yaacoub, Hassan Noura, Ola Salman, Ali Chehab. 2020. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, Volume 11 DOI: https://doi.org/10.1016/j.iot.2020.100218.

[3] Watkins, L., Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, W. H. Robinson, and A. Rubin. 2020. Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool. Workshop on Decentralized IoT Systems and Security (DISS) DOI: https://dx.doi.org/10.14722/diss.2020.23010

[4] Lanier Watkins, Juan Ramos, Gaetano Snow, Jessica Vallejo, William H. Robinson, Aviel D. Rubin, Joshua Ciocco, Felix Jedrzejewski, Jinglun Liu, and Chengyu Li. 2018. Exploiting Multi-Vendor Vulnerabilities as Back-Doors to Counter the Threat of Rogue Small Unmanned Aerial Systems. In Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy (Mobile IoT SSP'18). Association for Computing Machinery, New York, NY, USA, Article 1, 1–6. DOI:https://doi.org/10.1145/3215466.321546

[5] M. Yahuza et.al. 2021. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. IEEE Access, vol. 9, pp. 57243-57270 DOI: 10.1109/ACCESS.2021.3072030.