Don't Steal my Drone: Catching Attackers with an Unmanned Aerial Vehicle Honeypot

Emmanouil Vasilomanolakis*, Jörg Daubert*, Dhanasekar Boopalan†, Max Mühlhäuser*
Telecooperation Lab, Technische Universität Darmstadt
Darmstadt, Germany
*{vasilomano, daubert, max}@tk.tu-darmstadt.de
†dhanasekar.boopalan@stud.tu-darmstadt.de

***Abstract*—The increased utilization of Unmanned Aerial Vehicles (UAVs) in both personal as well as commercial and public safety scenarios has also opened the door to adversaries. In more details, such malicious activities may include the hijacking of the UAV (and its cargo), the theft of private information stored in the device, etc. In this paper, we introduce the idea of a honeypot that is specifically designed for the protection of UAVs. The honeypot, which is also capable of running on small portable devices, e.g., a Raspberry Pi, emulates a number of UAV-specific and UAV-tailored protocols, making it possible to lure adversaries into attacking it. Our system can assist into detecting active attackers in a certain area as well as into shedding light into the adversaries' techniques for compromising UAVs.**

I. Introduction

Unmanned Aerial Vehicles (UAVs), commonly referred to as *drones*, have gained massive popularity in recent years. UAVs are used for personal purposes, e.g., taking pictures and videos, as well as professional applications, such as agricultural surveys and package deliveries. Furthermore, even mission critical operations including medication delivery services and health and safety inspections are performed with UAVs nowadays. As UAVs are computer-controlled systems with radio/wireless interfaces, attacks and attack scenarios against these systems are surfacing [2], [3]. For instance, these may include wiretapping and theft of data, mission interference, and even the theft or misuse of UAVs. To cope with this attack landscape, we propose the idea of a portable drone honeypot; a security mechanism which can emulate the protocols that are utilized by UAVs and lure attackers into it.

A honeypot is a system whose only value lies in being probed, attacked, and/or compromised [1]. In more details, such systems have no real production value, but instead they appear to be vulnerable and thus attractive to attackers. Honeypots can be classified to *low*-, *medium*- and *high*-interaction with respect to the level of interaction they offer to the adversary. On the one hand, *high*-interaction honeypots are real systems that exhibit certain vulnerabilities and are closely monitored. These systems, however, are very expensive to maintain and have the risk of getting compromised. On the other hand, *low*- and *medium*-interaction honeypots only *emulate* protocols (with a different granularity) and are easier to monitor and contain.

Traditionally, honeypots are utilized as an early warning defense mechanism, a method for studying adversaries and their techniques, as well as a way to reduce the attack surface of the monitored network [1]. On top of these functionalities, we argue that due to certain properties of the UAVs, namely the signal strength property and the ability of the UAV to quickly traverse an area, a drone honeypot introduces additional benefits. In particular, in a drone-attack scenario the adversary does not have to maintain visual of the target, but instead can rely on their signal strength (e.g., by utilizing a strong-signal antenna) for attacking and hijacking the drone. Therefore, we argue that a UAV honeypot is able not only to detect a drone attack but even mitigate it as long as: (i) it has a stronger signal than the actual drone (which for example can be achieved with proper antennas) and (ii) that is placed in a strategic location. This scenario is also illustrated in Figure 1.

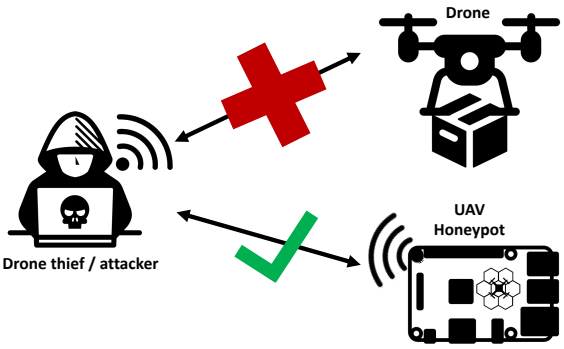

Fig. 1. High level view of the honeypot usage scenario

This paper proposes a novel *medium-interaction portable drone honeypot* that is able to:

- Provide a medium-interaction interface for many UAV-specific and UAV-tailored protocols,
- Record and analyze malicious activities in UAVs,
- Guide attackers away from UAVs and delay them, whilst reducing the overall attack surface of the monitored area.

II. A honeypot for UAVs

Today's UAVs often use commodity radio standards such as Wi-Fi and Bluetooth for command and control. Even vendor-

specific radio protocols, e.g., Lightbridge[1] and SiK Radio[2], operate frequency bands with a high availability of software-defined radios—ultimately making accessing UAVs easy for attackers. Additionally, UAVs use application protocols that have a long running track record of being attacked: Telnet, SSH, FTP, and more recently MAVLink[3]. Our portable drone honeypot leverages these properties to emulate drone radio interfaces on cheap commodity hardware, and by offering low to medium interaction and emulation for many of the aforesaid communication protocols. In addition, the mobile drone honeypot emulates all relevant properties for a range of commercial and self-build UAVs for command and control.

A number of state-of-the-art honeypots can monitor and emulate Wi-Fi connectivity, as well as some relevant protocols, such as Telnet, SSH, FTP [1]. However, only few honeypots have been designed to be mobile or portable [4]–[6], offering the ability to be placed close to the operating area of UAVs or mounted to a UAV directly. More significantly, to the best of our knowledge, no existing honeypot has been specifically designed to emulate radio and protocol properties of UAVs. Furthermore, there seems to be no honeypot supporting the MAVLink protocol.

The first generation of our portable drone honeypot runs on a Raspberry Pi, supports commodity Wi-Fi adapters, emulates the radios for AR Drones and MAVLink Wi-Fi telemetry drones. The honeypot emulates drone filesystems in combination with Telnet/SSH/FTP, and emulates MAVLink via the utilization of a drone simulator. Drone simulators were originally developed to train UAV pilots; these simulators realistically emulate a UAV's state including GPS coordinates, movement, and battery. As simulators are based on the control software of UAVs, these simulations provide a MAVLink interface and are virtually indistinguishable from a real UAV. All the attacker activity is logged into a database, including the possibility of replaying a flight (and attack) simulation.

With regard to the utilized technologies, the honeypot is using a Raspberry Pi, running Raspbian, in combination with an Alfa AWU036NH wireless adapter, and the Hostapd and Dnsmasq. The software is implemented in Python 2.7 and Twisted. A combination of PyMAVLink, MAVProxy and Ardupilot SITL simulates drones with MAVLink access. The honeypot takes UAV profiles from a configuration file and sets up all components to emulate a UAV down to Wi-Fi MAC addresses and UAV filesystems (contents extracted from real drones).

III. Demo Structure

In our demonstration, we plan to perform two realistic attack scenarios and subsequently show how our honeypot solution can detect or even mitigate the attack. The *first* scenario, will consist of a basic Wi-Fi de-authentication and hijacking attack in a Parrot AR Drone (connected to a smartphone), followed by a Telnet attack for the deletion of the UAV's internal files. Afterwards, we will activate the honeypot, repeat the attack and show the similarities with regard to the radio properties, the emulated filesystem, etc. The *second* attack scenario, will consist of an Arducopter (connected to a smartphone via MAVLink) which will be attacked via a Wi-Fi de-authentication attack. The adversary will then utilize MAVLink to redirect the drone to a new route. Thereupon, the honeypot will be activated and the same scenario will be repeated. In this case, however, the attacker will be lured by the honeypot and the hijacking attempt will be mitigated. This scenario is illustrated in Figure 2. Finally, in both scenarios we will present and discuss the logs that were recorded by the honeypot. The described live demo will also be accompanied by a poster and other relevant digital content, i.e., slides.

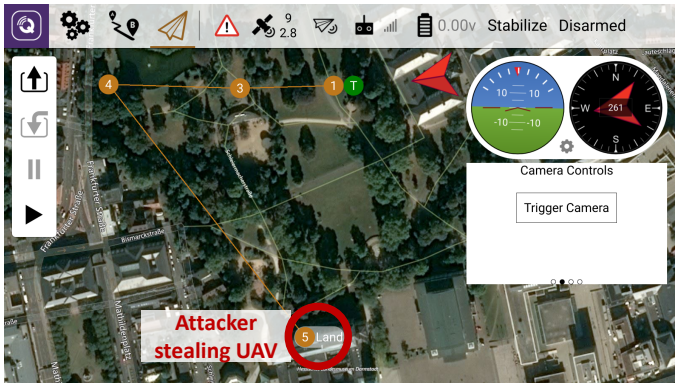

Fig. 2. Hijacking attack scenario

IV. Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No 700688.

[1] www.dji.com/lightbridge-2

[2] github.com/ArduPilot/SiK

[3] diydrones.com/profiles/blogs/hijacking-quadcopters-with-a-mavlink-exploit

References

[1] Marcin Nawrocki, Matthias Wählisch, Thomas C Schmidt, Christian Keil, and Jochen Schönfelder. A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249*, 2016.

[2] Johann-Sebastian Pleban, Ricardo Band, and Reiner Creutzburg. Hacking and securing the ar. drone 2.0 quadcopter: investigations for improving the security of a toy. In *IS&T/SPIE Electronic Imaging*, pages 90300L–90300L. International Society for Optics and Photonics, 2014.

[3] Nils Miro Rodday, Ricardo de O Schmidt, and Aiko Pras. Exploring security vulnerabilities of unmanned aerial vehicles. In *Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP*, pages 993–994. IEEE, 2016.

[4] E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Mühlhäuser. Multi-stage attack detection and signature generation with ics honeypots. In *NOMS 2016 - IEEE/IFIP Network Operations and Management Symposium*, pages 1227–1232, 2016.

[5] Emmanouil Vasilomanolakis, Shankar Karuppayah, Mathias Fischer, Max Mühlhäuser, Mihai Plasoianu, Lars Pandikow, and Wulf Pfeiffer. This network is infected: Hostage-a low-interaction honeypot for mobile devices. In *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices*, pages 43–48. ACM, 2013.

[6] Matthias Wählisch, Sebastian Trapp, Christian Keil, Jochen Schönfelder, Jochen Schiller, et al. First insights from a mobile honeypot. In *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 305–306. ACM, 2012.