Exploring Security Vulnerabilities of Unmanned Aerial Vehicles

Nils Miro Rodday, Ricardo de O. Schmidt and Aiko Pras
Design and Analysis of Communication Systems
University of Twente, the Netherlands
rodday@arcor.de, {r.schmidt,a.pras}@utwente.nl

***Abstract*—We are currently observing a significant increase in the popularity of Unmanned Aerial Vehicles (UAVs), popularly also known by their generic term drones. This is not only the case for recreational UAVs, that one can acquire for a few hundred dollars, but also for more sophisticated ones, namely professional UAVs, whereby the cost can reach several thousands of dollars. These professional UAVs are known to be largely employed in sensitive missions such as monitoring of critical infrastructures and operations by the police force. Given these applications, and in contrast to what we have been seeing for the case of recreational UAVs, one might assume that professional UAVs are strongly resilient to security threats. In this demo we prove such an assumption wrong by presenting the security gaps of a professional UAV, which is used for critical operations by police forces around the world. We demonstrate how one can exploit the identified security vulnerabilities, perform a Man-in-the-Middle attack, and inject control commands to interact with the compromised UAV. In addition, we discuss appropriate countermeasures to help improving the security and resilience of professional UAVs.**

I. Introduction

The fact that recreational Unmanned Aerial Vehicles (UAVs), accessible to the general public, are not secure is not new. Several papers and news articles have been published showing that one can easily hack into these devices [1] [2] [3]. However, recreational UAVs are hardly ever used for situations out of the leisure context. Examples of potential applications for professional UAVs are surveillance, border control and search & rescue. For sensitive and critical operations, professional UAVs are able to deliver the performance and functionalities that are needed. Examples of advanced features of these professional UAVs are long endurance and the ability to carry heavy payload. Clearly, the more advanced the more expensive the device is, and professional UAVs can easily cost several thousands of dollars.

Given the range of applicability, one should expect that security is a top priority for professional UAVs. From our analysis on a professional UAV, kindly borrowed from its manufacturer (names and models are not disclosed due to a non-disclosure agreement), we have learned that this is not the case. This puts critical operations for which these UAVs are used in danger of failure at the very least.

978-1-5090-0223-8/16/$31.00

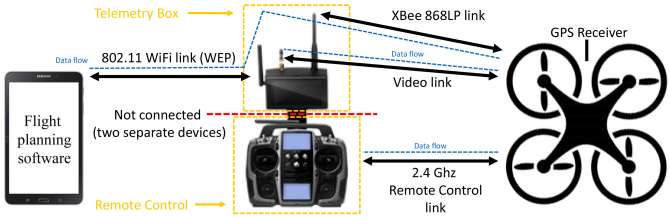

Fig. 1. Architecture

To the best of our knowledge, there is no work in the literature that openly addresses the security issues of professional UAVs. In this demo we show that professional UAVs are not as secure as one might expect. We demonstrate, that by learning how the UAV communicates with the remote controller, one can perform a Man-in-the-Middle (MitM) attack and potentially take control over the UAV, even at a distance of several kilometers from the actual UAV's controller. With our findings we raise awareness within (i) the general public that use and trust such professional UAVs, (ii) the scientific community by showing that further research is needed in this area, and (iii) the manufactures by showing the importance of implementing a higher level of security in their devices.

II. Exploring Security Flaws of the UAV

This research has been performed with a professional UAV, kindly borrowed from a high-end manufacturer. However, as the same hardware and software components are also used by other manufacturers, our approach and results can be extended to their respective UAVs.

A. System Architecture

Figure 1 shows that the UAV has telemetry, manual remote control (RC) and video links. The manual RC link uses common 2.4Ghz Graupner equipment and allows basic steering functionality within a range of 100m. The telemetry link allows for more advanced control features, such as setting way-points and automated flying. This is done from a tablet running the flight planning software which is connected via WiFi 802.11 to the telemetry box that in turn forwards the communication to the UAV by using XBee 868LP chips. The telemetry link can reach with a range of several kilometers much further than the manual RC link, allowing for full control of the UAV even if the UAV is far out of sight.

B. Security Vulnerabilities

We focused on the telemetry link of the UAV because of the broader range and the wider spectrum of control over the UAV. The telemetry link consists of two separate communication links, whereby the communication is forwarded between WiFi 802.11 and XBee 868LP by the telemetry box.

To communicate with an XBee 868LP chip the attacker needs to know the following connection parameters: PAN ID (network ID), BAUD rate, channel, destination high (DH) address and destination low (DL) address. PAN ID, BAUD rate and channel are all set to default values for every UAV and, hence, they can be considered of general knowledge. This way, a potential attacker still misses the DH and DL information. Theoretically, there are $\sim 18 \times 10^{18}$ possible combinations. However, the XBee 868LP chips respond to broadcast packets sent within their network, and this can be done through API-mode. The acknowledgement message for the broadcast contains the address of the sender, hence, revealing all available devices within the network.

Moreover, we have also identified a security gap in the WiFi link. The access point uses WEP (Wired Equivalent Privacy) as encryption scheme and can, therefore, be cracked. An attack on the WiFi link can be performed as follows: (1) crack the password, (2) disconnect the original user, and (3) connect the attackers tablet to the UAV. However, to do so, the attacker must be within the range of the WiFi link (100m), which likely makes such an attack too risky.

C. Man-in-the-Middle Attack

As shown in Figure 2, in order to perform a Man-in-the-Middle attack on the XBee 868LP chips we need to use "Remote AT Commands". This feature allows for the attacker to remotely change internal parameters of the XBee chips, such as DH and DL, and therefore reroute any traffic. The write command persists changes within memory, allowing for two different attack modes: temporary or persistent.

We have reversed-engineered both the flight computer and flight planning software. We were able to match commands transferred through the telemetry channel with specific functions within the UAV system. This enables an attacker to understand and alter existing packets in a meaningful way, or inject new packets to communicate with the flight computer.

D. Countermeasures

Fixing the security gaps we have identified within the studied UAV is not a straightforward procedure. First, secure encryption schemes should be used for the WiFi 802.11 access point connecting the tablet with the telemetry box. Second, data transferred through the XBee 868LP chip should not be sent in clear-text. Encryption should be used throughout the whole communication path. Three solutions could be employed: (1) XBee 868LP on-board encryption, which is the only solution that also mitigates the risk of Remote AT Commands, (2) dedicated hardware encryption in case the throughput drops significantly with XBee 868LP encryption, and (3) application layer encryption.

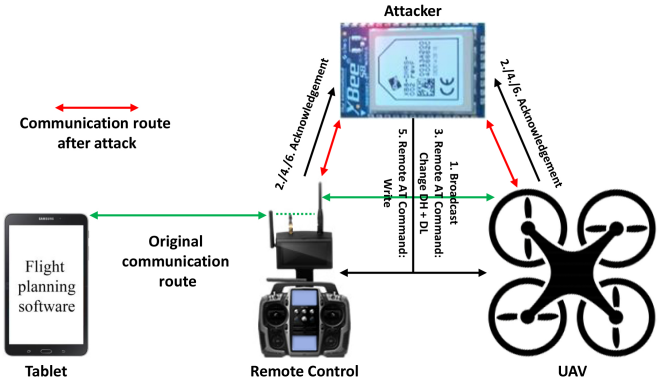

Fig. 2. Man-in-the-Middle attack

III. Final Considerations

In this paper we have shown that expensive professional UAVs can be hacked due to severe security vulnerabilities in their setup. We have shown that it is possible to effectively perform a Man-in-the-Middle attack from kilometers away by rerouting the traffic of the telemetry channel. Moreover, we have shown that by reverse-engineering the software involved in the communication of the UAV system, we can inject packets and control the UAV. Countermeasures to close these security vulnerabilities exist, but require the manufacturer to develop the system further and to patch every item sold so far.

IV. Demo Structure

We are going to present a live demo of the Man-in-the-Middle attack and control packet injection attack. The demo structure will consist out of the professional UAV we studied, the telemetry box and a tablet running the proper software to control the UAV. Moreover, the attacker will need a computer with a python interpreter installed, a common USB to RS232 adapter and an XBee 868LP chip to hack into the UAV and control it. There is no limit on the amount of times this demo can be replayed. The live demo will also be supported by an informative poster and/or slides.

Acknowledgment

The authors would like to thank Matthieu Paques and Ruud Verbij from KPMG Netherlands for their support.

References

[1] J. Pleban, R. Band, and R. Creutzburg, *Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy*, IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2014

[2] T. Fox-Brewster, *Maldrone: Watch Malware That Wants To Spread Its Wings Kill A Drone Mid-Flight*, Forbes Magazine, URL: http://www.forbes.com/sites/bernardmarr/2015/09/01/7-technology-trends-that-will-make-or-break-many-careers/, Visited on: 30.08.2015

[3] F. Samland, J. Fruth, M. Hildebrandt, T. Hoppe, & J. Dittmann, *AR. Drone: security threat analysis and exemplary attack to track persons.* In IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2012