Detection of Targeted Attacks Using Medium-Interaction Honeypot for Unmanned Aerial Vehicle

Abdul Majid Jamil[1(✉)], Hassan Jalil Hadi[1], Sifan Li[1], Yue Cao[1], Naveed Ahmed[2], Faisal Bashir Hussain[3], Chakkaphong Suthaputchakun[4], and Xinyuan Wang[5]

[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China
{majidjamil,yue.cao}@whu.edu.cn
[2] Prince Sultan University, Riyadh, Saudi Arabia
nahmed@psu.edu.sa
[3] Bahria University, Islamabad, Pakistan
fbashir.buic@bahria.edu.pk
[4] Bangkok University, Bangkok, Thailand
chakkaphong.s@bu.ac.th
[5] Zhejiang Scientific Research Institute of Transport, Hangzhou, China

Abstract. Over the last two decades, there has been significant growth in the drone industry with the emergence of Unmanned Aerial Vehicles (UAVs). Despite their affordability, the lack of security measures in commercial UAVs has led to numerous threats and vulnerabilities. In addition, software, and hardware complexity in UAVs also trigger privacy and security issues as well as cause critical challenges for government, industry and academia. Meanwhile, malicious activities have increased, including stealing confidential data from UAVs and hijacking UAVs. These attacks are not only illegitimate but also appear to be increasing in frequency and sophistication. In addition, the current defence mechanisms for counterattacks are not sustainable for two reasons: they either demand strict firmware updates for all of the system's devices, or they demand the deployment of a variety of advanced hardware and software. This paper proposes a Medium Interaction Honeypot-Based Intrusion Detection System (MIHIDS) to protect UAVs. Our system assists in detecting active intruders in a specific range (radio frequency) and provides details of attacking technologies to exploit UAVs. Our system is a passive lightweight, signature-based MIHIDS that is simple to integrate into UAV without requiring changes in network configuration or replacement of current hardware or software. The performance assessment demonstrates that in a typical network situation, our proposed framework can identify MitM, Brute-force, and DE-authentication attacks with a maximum detection time of 60 s. Under normal network scenarios, a minimum True Positive Rate (TPR) and performance efficiency is 93% to 95% during a short-distance detector.

Keywords: Unmanned Aerial Vehicle · Medium Interaction Honeypot · Intrusion Detection System

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 571, pp. 164–185, 2024.
https://doi.org/10.1007/978-3-031-56583-0_11