International Journal of Research in Engineering
www.engineeringpaper.net
Online ISSN: 2664-8784; Print ISSN: 2664-8776
Received: 25-10-2019; Accepted: 26-11-2019; Published: 27-12-2019
Volume 1; Issue 4; 2019; Page No. 32-34

Drone hacking-Spoofing attack on an unmanned aerial vehicle

Sudha VS[1], Sharada G Kulkarni[2], Shubhada S Kulkarnil[3], Gouri CK[4], Pankaja B Pati[5]
[1-5] Assistant Professor, Gogte Institute of Technology, Belagavi, Karnataka, India

DOI: https://doi.org/10.33545/26648776.2019.v1.i4a.24

Abstract
During the past years Unmanned Aerial Vehicle (UAV) usage has grown in military and civilian fields. Every year, emergency response operations are more and more dependent of these unmanned vehicles. Lacking direct human interference, the correction of onboard errors and security breaches is a growing concern in unmanned vehicles. One of the concerns raised by first responders using unmanned vehicles is the security and privacy of the victims they are rescuing. Video channels used for the control of unmanned vehicles are of particular importance, having great susceptibility to hijack, jamming and spoofing attacks. It is assumed the video feeds are not protected by any type of encryption and are therefore vulnerable to hacking and/or spoofing.

Keywords: unmanned, Vehicle, military, During

1. Introduction

THE Unmanned Aerial Vehicles were strictly military technology at first. Recently, UAVs have taken civilian responsibilities and are even used for fun by hobby enthusiasts. Even though UAVs are used widely for different operations their security is not what it should be and they are vulnerable devices. This makes them easy targets on both military and civilian fields. We concentrate specifically on the security of first responders unmanned vehicles and explore the possibility of obtaining the video feed. As demonstrated by [9] these unmanned vehicles can be jammed and spoofed, but is the video feed accessible? Obtaining the video feed can be a violation of privacy for civilians and can put a first responder's life at risk in certain situations. This is the question we set out to answer at the beginning of summer and to study the vulnerabilities of UAVs from a cyber-security perspective. In this report different weak points in the drones are examined and considered. Several previous incidents and experiments with UAV security are discussed

2. Components of UAVS

The Autopilot system was directly transferred from manned vehicles to unmanned vehicles without barely any changes [3], this renders it vulnerable to attacks that had previously not been considered in the case of manned flight. The autopilot has many components that are all dependent on each other. Any corruption of any of the components may result catastrophic
to the flight path and to the UAV. Among the components of the autopilot are: • GPS • Magnetometer • Internal Measurement Unit • Actuators • Manual Controls These components are all at risk of attacks from external sources and affecting greatly the vehicle. The drone's GPS receiver is one of the biggest weaknesses, being dependent on the unencrypted civilian GPS. This means the GPS signals are easily spoofed like it has been before [9]. The Magnetometer is used for measuring direction and it gets information from other sensors on the drone. If fed wrong information the drone could alter its flight path and go somewhere else or change altitude or direction. The same concept applies to the Internal Measurement Unit, which is in charge of measuring the movement of the drone. The actuators receive information from the main processing board, which in turn receives all the inputs from all the sensors and pre-loaded and curre….nt commands of the drones and gives a navigation path for the drone to follow. The actuator is the next to last step on delivering the flight path of the aircraft. This makes the actuators a very likely target and their protection should be secure. The actuators could be affected by a denial of service attack or a malicious data injection attack, both resulting in damaging behavior to the UAV. Unmanned Aerial Vehicles are no strangers to wireless attacks as demonstrated by previous attacks. The UT Austin Radionavigation laboratory has successfully spoofed drones [9]. The techniques of spoofing and jamming are no new thing and are known among certain circles. Anti spoofing techniques such as checking that a signal does not exceed a certain bandwidth are not always reliable. Not only GPS sensors can be attacked with this method but also the vision, radar and infrared sensors can be spoofed and jammed in an attack like this. As a result, the UAV's flight path might be affected and it might become erratic. If the UAV is being control manually by a ground control station the video feed is the only way the conductor knows where the UAV is headed. In the event of the video signal being compromised the controller no longer knows where he/she is driving the UAV to. Specifically, when the GPS and ADS-B (a device that every flying device will soon be equipped with and broadcasts the location to nearby aircraft to avoid collision) are spoofed the drone can be made believe that it is not where it is or that a collision is imminent or that there are no incoming aircraft. This will cause the drone to change it's flight path to avoid collision, causing erratic and unexpected behavior which can cause the drone to crash and/or land in the hands of the enemy.

3. Methodology

For this project two unmanned vehicles used by first responders were considered: The Dragon Runner and the Air Robot AR100-B. According to the spec sheet the Air Robot AR100B has a video feed at 2.4GHz and control feeds at 925MHz. The Dragon Runner transmits in a range from 2.4016GHz to 2.482GHz according to its specs. A Tektronix SA2500 handheld spectrum analyzer was utilized to scout the spectrum for the signals from these unmanned vehicles. Since the unmanned vehicles transmitted at around the same frequencies of Wi-Fi we considered the 802.11 and 802.15 protocols to be the potential ones that are used between the control station and the vehicles. Another potential frequency identified was 5.0GHz, as other drones transmit in this frequency. First we took a look at the Dragon Runner. This part of the spectrum was crowded with a lot of WiFi signals but we were able to find the video feed signal (not obtain it). The video feed was found at a frequency of 2.422GHz. Later on we tried with the Air Robot, we were unable to find the frequencies at 2.4GHz on two separate occasions. The specs for the robot say the video feed signal is at 2.4GHz. The spectrum analyzer provided us with a look into the signals but it was not able to provide us with the actual data feed. For that, a wireless video receiver will be needed. Several options for video feed receivers in the 2.4GHz range were considered but due to time constraints they were not applied. What was obtained was a data log for the video feed, what we thought (at the time) that it was the video feed. We tried to find the pattern and uncode it but it proved to be not the way to go since data log did not equal video feed.

4. Security Issues

A. Incidents where UAVs have been compromised

During the past decade several incidents have made clear that unmanned vehicles are not invulnerable and that some security issues need to be addressed. The events have been both in the military and civilian fields. On 2009 a U.S. military drone's video feed was intercepted by Iraqis militants. It goes without saying that the the mission's and soldier's security had been compromised. What was the most alarming thing was that the Iraqi military had used an off the shelf software to capture the video feeds [1, 2]. At this time a large amount of the US's military drone fleet was not properly encrypted and it has been said by the Pentagon that the proper precautions have been taken since then. The Sky Grabber software is an off the shelf product mainly used to intercept satellite feeds of music, tv, videos, etc. At the time the owner of the software was not aware of the potential to capture drone video feeds using his software. It is said that at the time the US military was aware that the drones video feeds were unencrypted and easily accessible but had not addressed the issue because they were hoping to change platforms (of drones) and the new platform would have encryption [2]. This event put a dent on the trust people had on drones and made it clear that they are a target and can be an easy one at that. In figure 1 we see how the Sky Grabber was able to obtain the video feeds from drones

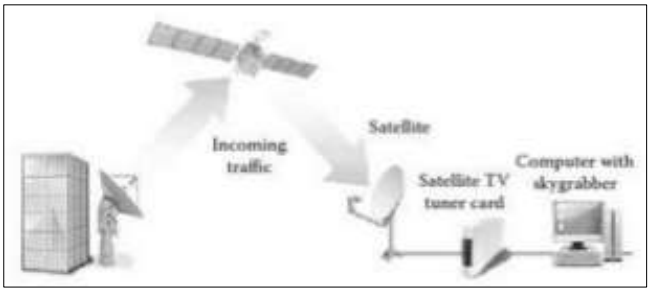

Fig 1: Diagram demonstrating how obtaining video feeds from drones using SkyGrabber was possible [2]

Another noticeable incident occurred in 2011 when a key logger virus infected an Air Force Base's computer [4]. On 2011 a key logger virus was discovered on the computers of the Creech Air Force Base. Supposedly, the virus was not deemed that worrisome and did not feed information to any outside sources, the Air Force later reported. The virus got there by means of external hard drives or unauthorized uses of the computer. Even if these computers run outside the internet, it doesn't make them completely invulnerable. The keylogger virus tracked every stroke made by the military personnel on the computers. These computers are used to specifically manage the drone fleet over Iraq and Afghanistan. The military was lucky that this incident did not put in jeopardy any missions or military personnel lives. One of the biggest vulnerabilities to civilian UAVs is spoofing. As demonstrated by the UT Austin's Radio Navigation Lab [9] it is easily achieved with several pieces of equipment. One of the biggest reasons spoofing is possible is because civilian GPS is not encrypted and the documentation is publicly available. Encrypting the civilian GPS would implicate a severe modification to the infrastructure and a big investment that could take years to implement. It is not guaranteed that this will be done in the future. When spoofing an unmanned vehicle the person takes over the incoming GPS signals the vehicle is receiving and is able to control which way it goes. It can be done covertly or overtly, the former being the hardest method to do. In both cases the pilot loses total control of the unmanned vehicle and might be impossible to regain it. If anyone wishes to spoof the vehicle the equipment is expensive but readily accessible, making spoofing a real threat to civilian vehicles. Civilian drones are even more vulnerable to attack, as has already been proven. Just when companies like Amazon and FedEx were announcing that they might start experimenting with drones delivering their packages, Sammy Kamkar, released Sky Jack, a software meant to take control of drones using another drone [5]. Sky Jack is not applicable to every drone, it is only applicable to drones being controlled over a WiFi network. The code can be run from another drone or from a ground linux machine within range of the drone to be taken over. The drone or computer identify a drone to be taken over and forcefully disconnect it from its legit ground control station then it takes over the signal, giving the hacker full

control over the drone. This attack is not passive at all and the other person will know the attack took place. Drones have also been used to attack civilian's electronic devices. This past year, Snoopy [8], a distributed tracking and profiling framework was unveiled. This software can be put airborne by drones and it takes advantages of the different electronic devices hailing for WiFi networks. It can also read Radio Frequency Identification (RFID), Bluetooth and 802.15 [7]. Posing as an already recognized network the drone can successfully obtain personal information from the person and track the person's whereabouts. It can access cellphone data and all the data and requests transmitted over the network. This last security breach is interesting because it can be used for first responder emergencies. A drone with the software can be developed over an area and it can track the movements of cellphones or other electronics in the area, or maybe whether they have moved or been active in the past hours or so. Feeding this information to first responders may help them identify areas where survivors are and plan accordingly to rescue them.

5. Future work

In the future we hope to expand our work by obtaining the video feed. Several options of video receivers could be tested and see if they work with the drones or one could be built. If it proves to be unencrypted, working on the encryption of the video feed is paramount to protect if from unwanted eyes. For the internal parts of the UAV a lightweight software that checks for abnormalities to prevent data injection attacks among the components is also essential. When one of the pieces of the drone has been compromised, all of it becomes compromised and a risk. Inputs such as the GPS, ADS-B, infrared camera and magnetometer (if equipped with any of those) should be unspoofable or at least the drone should be able to recognise something is off with it's pre assigned flight path and what it is receiving. Or correlate with other sensors on board. The biggest challenge is encrypting civilian GPS since it means a large update to the infrastructure and a lot of money. There are ways to detect a counterfeit signal, but those are not guaranteed to ward off a very sophisticated spoofing attack. They mainly depend on the strength and noise of the signal, if it exceeds a certain threshold it raises alarm and it means the drone is probably being spoofed. Perhaps in the future this method can be more sensitive and improved agains spoofing attacks.

6. Conclusion

In the future, unmanned vehicles will play important roles in our society. From delivering your mail to mapping an area to unarming a bomb, they will become essential. Although, encrypting the civilian GPS will make a spoofer's job harder it is a momentous project that will take years to implement. As for the video and control feed encryption and security it is an issue that needs to be addressed as soon as possible by the manufacturers. In this project we found the frequencies of the video feeds with a spectrum analyzer. We were also able to obtain the frequencies of the control feeds. For now, we have not been successful at obtaining the video feed but several viable options were identified that can be explored in the future.

7. References

1. Gorman S, et al."Insurgents Hack U.S. Drones" Internet: http://www.online.wsj.com/news/articles/SB126102247889095011, Dec 7, 2009, 2014.
2. McBride SP. Pirating the Ultimate Killer App: Hacking Unmanned Military Aerial Vehicles in Information Security Management Handbook, 6th ed, Vol. 6. H.F. Tipton, M.K. Nozaki, Auerbach Publications, 2012, 301-316.
3. Kim Alan, et al." Cyber-attack vulnerabilities analysis for unmanned aerial vehicles." The American Institute of Aeronautics and Astronautics: Reston, VA, USA, 2012.
4. Shachtman N." Exclusive: Computer Virus Hits U.S. Drone Fleet" Internet: http://www.wired.com/2011/10/virus-hits-drone-fleet/, Oct. 7, 2011, 2014.
5. Crook J." Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones" Internet: http://techcrunch.com/2013/12/04/infamoushacker-creates-skyjack-to-hunt-hack-and-control-other-drones/,2013, 2014.
6. Kamkar S." Sky Jack" Internet: https://github.com/samyk/skyjack, 2013. [Aug. 5, 2014].
7. Goodin D." Meet Snoopy: The DIY drone that tracks your devices just about anywhere" Internet: http://arstechnica.com/security/2014/03/meetsnoopy-the-diy-drone-that-tracks-your-devices-just-about-anywhere/, 2014. [Aug. 5, 2014].
8. "Snoopy" Internet: https://github.com/sensepost/Snoopy [Aug. 5, 2014]
9. Kerns Andrew J, et al." Unmanned aircraft capture and control via GPS spoofing." Journal of Field Robotics, 2014.