Analysis of Vulnerabilities in Modern Unmanned Aircraft Systems

Nikolas Shashok

December 13, 2017

Abstract

As unmanned aerial vehicles (or drones) become more prevalent in modern society, it is crucial that an understanding of the vulnerabilities present in drones becomes more widespread. This paper will discuss some of the modern uses of drones and the possible risks inherent in their use, and will go into detail on a number of vulnerabilities present in drones today, including GPS spoofing and jamming, drone-specific malware, and data extraction and reverse engineering. The goal of this paper is to build a basic and general awareness of drone cybersecurity issues today, for both cybersecurity professionals and everyday users.

1 Introduction

In 2012, a research team working at the University of Texas Cockrell School of Engineering achieved a previously unknown feat: they successfully managed to interfere with and remotely control an unmanned aerial vehicle simply by falsifying the GPS signal it was using to maintain its position. This technique, known as GPS spoofing, was performed without interacting directly with the drone at all. In another case, a developer created a "drone vampire" which flies to other drones and takes control by exploiting the little to no security present on many consumer drones – a problem we've seen before in Internet-of-Things devices. Drone security is becoming steadily more important as more industries pick up drones for various tasks, and it is crucial that as they spread, we do not fall into the same traps we have fallen into before. Thus, what are some of the most common vulnerabilities that modern drones suffer from today?

1.1 What Is a Drone?

Colloquially known as drones, unmanned aerial vehicles (UAV) are defined as "[any] aircraft that does not carry a human operator and is capable of flight with or without human remote control." [8] This paper will use the terms "unmanned aerial vehicle", "UAV", and "drone" interchangeably. UAVs form one component of unmanned aircraft systems (UAS), which also include the operator of said aircraft, and the system of communication between the two. The term UAV covers a wide spectrum of different vehicles including single-rotor, multi-rotor, fixed-wing, and balloon aircraft, over civilian, commercial, and military uses.

2 To The Community: Modern Drone Uses and Risks

When most people think of drones, they will consider the simple quadcopters people are using to make sports videos, or the military UAVs used to remotely bomb targets of interest. However, as drones get smaller, cheaper, and smarter, their possible uses continue to increase, possibly placing a wide variety of industries at risk if drone security vulnerabilities fly–pardon the pun–under the radar.

2.1 Civilian Drones

One of the simplest and most common uses for drones is hobbyists looking to fly recreationally. The Federal Aviation Administration does not require recreational fliers to register their drones if they meet a size requirement and the user maintains line-of-sight at all times. There also exist a number of location-based requirements that the user does not fly close to airports, certain public spaces, and other locations where the drone might cause disturbance. The amount of damage a recreational drone can do is small, but there have been

cases of drones interfering with aircraft or crashing into sporting stadiums. It is possible that a compromised hobbyist drone could cause property damage or severe injuries. Along a similar vein are sport filming drones, designed to be semi-autonomous and track skiers, bikers, and other solo athletes. When compromised, these drones could cause similar physical damage, but as many models will store video data on-board, there is an additional risk of private data being compromised.

2.2 Commercial Drones

Commercial uses for drones range from news filming to package delivery, and this opens up a large field of possibly compromised industries. Amazon is currently pushing for rollout of Prime Air, a service that will allow packages to be delivered quickly using Amazon-owned UAVs. The FAA has published regulations that prevent Amazon from testing this service in the US with any efficiency, but tests are being carried out in other countries with no such regulations. If a Prime Air drone is compromised, the attacker could of course steal whatever packages it is carrying by piloting it to the attacker. Additionally, the attacker could obtain address information about the package's recipient, and possibly payment or account information as well. Another, possibly more drastic example, is drones being used to map and help extinguish wildfires. There are two sides to this coin: firefighters have already had trouble with hobbyist drones getting in the way of emergency helicopters and preventing safe approach, and compromised drones could do the same without the original users' intent. Additionally, a compromised firefighting drone could both interfere with human-piloted vehicles and remove an important source of information for analyzing the fire. This goes hand-in-hand with other forms of emergency response conducted by drones; a compromise means a loss of crucial information. Finally, Facebook has been conducting tests of an experimental solar-powered drone designed to provide Internet to low-connectivity regions. Besides the normal risks of a fully autonomous drone being compromised, this drone now has to deal with the vulnerabilities inherently present in any Internet hub, including encryption, data interference, and denial-of-service attacks. Compromising this drone could also shut down essential communication infrastructure in said low-connectivity regions, especially if that infrastructure is being used for emergency response.

2.3 Military and Law Enforcement Drones

Military drones are terrifying as they are, even without the risk of them being compromised by malicious organizations. Some of the most common uses of drones today are for military or law enforcement purposes, including reconnaissance, telecommunication, search and rescue, disaster management, and munitions. [9] Importantly, although (and because) these types of drones pose a much greater threat on their own, the security is much tighter on them, making it much more difficult for an attacker to manipulate them; for example, the military GPS ranging codes are encrypted using a method kept tightly under

wraps, and so an attacker would have to break this encryption to generate a compatible code.

3 Common Vulnerabilities

3.1 Indirect Attacks and GPS Interference

Many autonomous or semi-autonomous drones will use GPS to position themselves and move relative to the Earth. This connection can be exploited to make the drone lose its orientation or even trick it into adjusting itself to a new, malicious orientation.

3.1.1 How does GPS work?

Briefly, GPS works by a set of satellites constantly broadcasting a weak signal about the satellites' positions, time information, and status about the GPS network. This signal is constructed from a carrier wave at a set frequency and a data signal which is added to the carrier using binary phase-shift keying (BPSK), a technique which uses a 180°phase shift in the carrier to represent high (1) and no phase shift to represent low (0). GPS receivers will pick up this information, but they will not send information back; thus, the protocol is connectionless. Receivers will use the location and time data to triangulate their own position. There are two main sets of ranging codes that the satellites broadcast: coarse/acquisition, which is used for public applications, and precision, which is encrypted and used for military applications. Many autonomous or semi-autonomous drones will use GPS information to determine altitude and latitude/longitude information, and will adjust themselves accordingly if they detect a deviation from the desired position.

3.1.2 GPS Jamming

GPS jamming is the practice of generating useless or noisy signals that interfere with GPS receivers' ability to pick up legitimate signals. By broadcasting a noisy signal at a greater strength than a legitimate signal, the receiver will be unable to distinguish the real signal from the noise, and so will be unable to function. [5] This is fairly simple to do, as the signal strength of legitimate GPS signals is very low. There are a number of ways to generate noisy signals: by using a continuous wave jammer, which simply rebroadcasts the GPS carrier frequency with no modulation (i.e. a signal with all zeros), or by using a noise jammer, which adds random noise to the carrier signal. Both techniques are effective. GPS jamming–and signal jamming in general–is illegal in the United States, as jammers can interfere with emergency response and other critical communication networks. However, GPS jammers are fairly simple to make, and there are many online stores which claim to sell them–some even go so far as to make ones specifically tailored towards drones, which are fairly susceptible as jamming signals travel farther without line-of-sight blockages. When civilian

drones lose the GPS signal, many of them will simply drift with the wind, as they can no longer maintain their position with accuracy; thus, a jamming attack will not guarantee the attacker will be able to gain control or even retrieve a downed drone. However, these attacks can disrupt normal operations, which is dangerous in cases where the drone is gathering sensitive data.

3.1.3 GPS Spoofing

The bigger and meaner cousin of GPS jamming is GPS spoofing, where the attacker creates a GPS signal which conforms to the GPS standard but contains incorrect information on satellite position or current time. This signal can then override legitimate GPS signals and trick a drone into adjusting its position to match the false position information. In 2011, Iran claimed that their engineers had used GPS spoofing to force a United States RQ-170 military drone to land in the wrong location, allowing them to retrieve it. [10] While this was theorized to be possible, one of the most prominent demonstrations was not created until 2012, when a group of researchers from the University of Texas Cockrell School of Engineering used a custom-built GPS spoofer to successfully target and bring down a UT-owned Hornet Mini consumer drone. [1] Their attack strategy was as follows: first, they calibrated the spoofer by receiving legitimate civilian GPS signals, creating a false data-free signal, and measuring the delay between the two. When the spoofer was calibrated, they began broadcasting the false signal, initially in sync with the legitimate signal but with a lower power. They then raised the power of the false signal above that of the legitimate signal, meaning the drone being targeted was now under the attacker's control. Finally, by slowly diverging the false signal from the drone's real position, they were able to trick the drone into self-adjusting based on the incorrect position information. When testing on the Hornet Mini, the group told the drone to hover at a set altitude, then created a false velocity that caused the drone to self-correct and move in the opposite direction. Of note is the fact that when a drone is being controlled through GPS spoofing, the normal self-correcting abilities of the drone are disabled, as the false signal does not take into account any random movement the drone makes. Thus, the attacker must control the drone directly, which requires a high level of GPS precision. Having proved that GPS spoofing of a sophisticated civilian drone was indeed possible, members of the group went on to use the same technique to draw a private yacht off course in 2013. [6] By inducing subtle deviations from the yacht's intended path, the team was able to cause the computer to call for course corrections, but it was the crew of the yacht that had to–and in fact did–act on those corrections. This demonstration proved that even when the vehicle is not fully autonomous, GPS spoofing can still lead the pilot astray. Spoofed GPS signals are much harder to detect than jamming signals, as they conform to the GPS standard and for all intents and purposes look legitimate; thus, spoofing attacks are far more dangerous than jamming attacks are, and the two can be used in conjunction to great effect. Additionally, while the encrypted military GPS codes are far more difficult to spoof directly, if the drone being attacked is programmed to fall back on civilian

codes if the military codes are unavailable, spoofing attacks are still possible by jamming the military channel and broadcasting a spoofed signal on the civilian one; this is how Iran was theorized to perform its attack.

3.2 Direct Attacks and Malware

GPS attacks are effective without directly accessing any part of the drone, and when the drone is fully autonomous; however, they do not provide direct control over the drone's behaviors when the drone is manually piloted, and cannot access any data. To this effect, examples of drone WiFi cracking and drone-specific malware have been cropping up over the past decade, which directly affect the drones being attacked.

3.2.1 WiFi Cracking

In 2015, a graduate student at the University of Twente analyzed a group of direct vulnerabilities in a professional UAV for their master thesis; as part of their analysis, they successfully took control of the drone by breaking into its wireless connection with the controller. [7] The drone in question was controlled by a telemetry box, which receives flight data from a WEP-encrypted WiFi-connected tablet. By falsely authenticating and associating the attacking computer with the network, the student was able to capture traffic from the network and generate false traffic which would be accepted by the access point. The student then cracked the password for the access point, connected a malicious controller tablet to it, and was able to control the telemetry box as a malicious user. This was possible due to the security vulnerabilities present in WEP; at the time, the student suggested switching to WPA2 for increased security, but as WPA2 has now been shown to be vulnerable as well, even more secure wireless connections could be compromised using the known WPA2 exploit. Thus, any drone controller system that can receive data using WiFi is potentially vulnerable, given the attacker is in close proximity to the access point for the controller.

3.2.2 SkyJack

In order to solve the issue of an attacker needing to be near the access point to infiltrate the drone, an independent developer created SkyJack, a drone designed to autonomously seek out and take over other drones. [4] SkyJack will search for wireless access points being transmitted by drones in the area (specifically, the Parrot AR.Drone, a particularly vulnerable model which uses an unauthenticated unencrypted access point that users use to control the drone via smartphone). It will then navigate near to them, then send deauthentication packets to trick the drone into thinking the controller has disconnected. SkyJack then reauthenticates with itself as the controller. Once SkyJack has control, the attacker can send control signals to it which it will forward to any

drones it has control of. While this attack only targets a small variety of appallingly vulnerable drone models, it is very cheap to make, requiring only a Raspberry Pi, specialized network cards, and the same model of drone being attacked. This also provides a good example of why devices like this need to be properly secured regardless of their status as a "toy" or "novelty".

3.2.3 Maldrone

Now that drones can be maliciously accessed directly, this opens up the prospect of malware being installed covertly. To this effect, an independent developer created Maldrone in 2015, which he claims is the "first ever drone backdoor". [3] Maldrone is an exploit designed to run on the same Parrot AR.Drone model which SkyJack attacks, and the developer even recommends pairing the two. This model of drone uses a set of internal serial ports to receive data from and send commands to peripherals such as the GPS, accelerometer, other sensors, and rotors. Maldrone temporarily disables the control program using those serial ports, then sets up a set of proxy ports which it controls. It then reenables the control program, which connects to the proxy ports, and begins acting as a man-in-the-middle attacker, listening to traffic from the real ports and forwarding both legitimate and falsified signals to the control program. Paired with Skyjack, this has the potential effect of Parrot AR.Drone models becoming infected without the user realizing, and being controlled remotely by the attacker while still maintaining a facade of control.

3.3 Data Extraction and Reverse Engineering

The direct attacks described above involve using a well-known set of vulnerabilities in a well-known protocol, namely WiFi. Many drones use proprietary methods to communicate with the controller, and these need to be reverse-engineered before an attacker can take control of the drone. Additionally, it may be difficult for an attacker to extract data from a captured drone once they have it.

3.3.1 Iranian Reverse Engineering

In addition to claiming their engineers had in 2011 used GPS spoofing to bring down a RQ-170 military drone, Iran also claimed they had successfully extracted data from said drone. Apparently they had found maintenance schedules, flight data, and other possibly compromising information. Much like the claims from the original incident, there is little evidence of this being true; however, the prospect is distressing. The best solution to data extraction from captured drones is to not let drones be captured in the first place; the next best thing is to encrypt all information the drone collects and requires to operate.

3.3.2 XBee and Proprietary Radio Cracking

As part of their analysis, the student from the University of Twente also analyzed the radio connection between the professional drone and the telemetry box. The drone in question used a radio chip called XBee, which is present in a wide variety of consumer drones and drone kits, as it is very cheap. The chip uses the radio frequency bands between 836 and 870 MHz. In order for two chips to communicate, the UAV chip needs to know the device addresses of the controller chip, and vice versa; these addresses are written on the chips, but can also be brute-forced or deduced by listening into the correct channel and reverse-engineering the packet structure. Once the attacker has the address of the UAV chip, the attacker can send a particular command that alters the destination address of the UAV chip, thus allowing the attacker to communicate with the chip directly; this change persists until the drone restarts, or can be made permanent by sending a write command. Now the attacker has direct communication with the drone, but does not know the packet structure. By changing the destination addresses of both the UAV chip and the controller chip, the attacker can act as a man-in-the-middle and capture all traffic for analysis while forwarding it to continue normal behavior.

3.3.3 Controller App Reverse-Engineering

While it is possible to reverse-engineer the XBee packet structure directly, by lots of trial and error, the student also analyzed the method of reverse-engineering the Android application being used as the controller. The student used the dex2jar tool to transform the classes.dex file present in the application's APK into a .jar archive, which contains the set of Java classes in standard Java format. They then used JD-GUI to view the class files in an organized manner. By doing so, the student determined the format of the commands as they were sent to the Android network chip, then used this knowledge in conjunction with the traffic monitoring mentioned earlier to deduce the correct command codes for "start engines" and "auto-takeoff". This reverse-engineering technique saved a great deal of time, effort, and physical proximity to the target, and could be accomplished with any drone that uses an Android application to receive commands.

4 Call to Action

Given this large variety of different drone exploits, what can we do to prevent disaster? A number of possible fixes exist already or are in the works, and a number of others are possible with current or near-current technology. GPS jamming is easily detected, as both methods of jamming use junk data patterns which are not properly synced with the GPS standard pseudo-random codes; these can be checked for. It may be possible to add a certification method to civilian GPS signals which involves adding cryptographic signatures to legitimate messages; this would help to prevent spoofing, as an attacker would

have to crack the signatures before fabricating messages, and in addition could help prevent GPS time spoofing as well. For the purpose of securing consumer drones, it is imperative that manufacturers treat the drones they are making as potential security risks and secure them accordingly using up-to-date standards; the SkyJack exploit would not have been possible had the manufacturers used WPA2 or another (reasonably) secure wireless authentication method. Encryption of proprietary radio protocols like XBee is also a reasonable solution, either at the device layer or the application layer, to prevent reverse engineering of control codes. Finally, one of the best methods is simply spreading awareness of drone security; if drones continue to spread as they have, it is crucial that the drone industry does not fall into the same trap the Internet of Things industry fell into.

5 In Summary

As drones continue to make their way into modern society, we must continue to investigate and build on our knowledge of their risks and vulnerabilities. Drones span such a wide range of industries and uses that to fail to consider the risks will cause a great deal of damage. What we know right now: drone vulnerabilities range from the simple and cheap, such as GPS jammers, drone-specific malware, and insecure wireless access points, to the esoteric and dangerous, such as GPS spoofing and the risk of reverse-engineering. Already, there have been large-scale examples of drones being taken over, some by researchers and some by potentially malicious agents. Thus, cybersecurity professionals and everyday users alike must stay alert for vulnerabilities in the modern UAV.

6 References

[1]D. Shepard, J. Bhatti, T. Humphreys and A. Fansler, Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. Nashville: 2012 ION GNSS Conference, 2012.

[2]"Iran says it has gleaned data from U.S. spy drone", SFGate, 2012. [Online]. Available: http://www.sfgate.com/world/article/Iran-says-it-has-gleaned-data-from-U-S-spy-drone-3501847.php. [Accessed: 02- Nov- 2017].

[3]R. Sasi, "Maldrone the First Backdoor for drones. - Blogs - Garage4hackers Forum", Garage4hackers Forum, 2015. [Online]. [Accessed: 02- Nov- 2017].

[4]S. Kamkar, "SkyJack: autonomous drone hacking", Samy.pl, 2013. [Online]. Available: http://samy.pl/skyjack/. [Accessed: 02- Nov- 2017].

[5]A. Purwar, D. Joshi and V. Chaubey, "GPS signal jamming and anti-jamming strategy — A theoretical analysis - IEEE Conference Publication", IEEExplore, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7838933/. [Accessed: 02- Nov- 2017].

[6]A. Lee, "UT Austin Researchers Spoof Superyacht at Sea - Cockrell School of Engineering", Engr.utexas.edu, 2013. [Online]. [Accessed: 02- Nov- 2017].

[7]N. Rodday, Exploring Security Vulnerabilities of Unmanned Aerial Vehicles. Amsterdam: University of Twente, 2015.

[8]"Unmanned Aircraft", DOD Dictionary of Military and Associated Terms. Department of Defense, 2017

[9]"Unmanned Aerial Vehicle Systems Association Military Applications", UAVS.org, 2017. [Online]. Available: https://www.uavs.org/military. [Accessed: 12-Dec-2017]

[10]C. Mackenzie and M. Duell, "'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil", Daily Mail Online, 2017. [Online]. Available: http://www.dailymail.co.uk/news/article-2075157/Iran-claims-hacked-US-spy-planes-GPS-guided-aircraft-ground.html. [Accessed: 13- Dec- 2017].