ISSA
DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Drone Hacking: Mirai in the Sky?

By Clara Andress – ISSA member, Puget Sound Chapter
and Jason Andress – ISSA Senior Member, Puget Sound Chapter

This article covers some of the security issues surrounding drones and drone hacking. Discussed are vectors that might be used to scale these up to a Mirai-style attack and some of the steps that could be taken to mitigate such issues.

Drones are everywhere. We see them in the news media daily and in nearly every toy and department store. Commercially they are used to take sweeping aerial shots in movies and imminently for package delivery [1] [2]. They are used in areas too dangerous for fragile humans to enter, such as reconnaissance for fighting the fires at Notre Dame[1] or in delivering over 2,600 air strikes in Afghanistan in 2017 [3]. With the increased use of drones commercially and high adoption rates for recreational use, the number of drones has grown exponentially over the last few years. The FAA predicted the count to reach 3.1 million by the year 2022, almost tripling the number of drones registered in 2017 [4].

Drones generally consist of four major parts: the platform, sensors, the flight control system (FCS), and external communication systems as shown in figure 1.

The platform is the part of the system that does the physical work of movement and carries all of its other components. These include things such as the chassis, power supply, landing gear, antennas, and motors. The US DoD classified drones into five groups: UAS 1-5, from aircraft weighing less than 20 pounds to those that weigh over 1,300 pounds, with a wide range of operating altitudes and airspeeds [5].

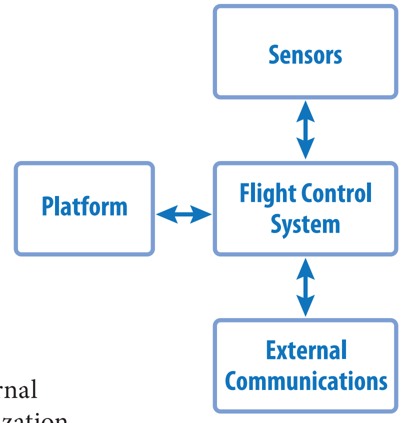

Figure 1 – Drone systems

Sensors collect data for the flight control system to act on. Some sensors collect internal data, such as gyro stabilization, inertial measurement units, tilt sensors, and internal compass. Other sensors collect external data like GPS, cameras, infrared, and chemical sensors.

The data collected by the sensors is sent to the **flight control system** (FCS). A portion of the FCS on many drones resides outside of the device itself in mobile applications, ground control systems, and backend systems. The drone uses its **communication systems** that may take advantage of many radio frequency (RF) technologies, such as Wi-Fi, Xbee, 4G/LTE, and other RF-based video and control signals, as well as satellite-based technologies such as global positioning system (GPS).

[1] Tom Nardi, "The Drones and Robots That Helped Save Notre Dame," Hackaday.com – https://hackaday.com/2019/04/17/the-drones-and-robots-that-helped-save-notre-dame/.

With the increased availability and reduced price of recreational drones, they are becoming more accessible for the hobbyist to purchase for personal use. The Federal Aviation Administration (FAA) requires all drones to be registered, which costs $5 for three years. Additionally, there is new legislation, the FAA Reauthorization Act of 2018, that would require drone operators to pass an online aeronautical knowledge and safety test and carry proof of test passage. This law is planned to go into effect in the summer of 2019 [6].

Security issues surrounding drones

As with any new technology, there are a number of security issues surrounding drone technology and the use of it, primarily in the areas of integrity and availability. Although this is by no means an exhaustive discussion, we will cover a few of the more salient issues here.

Airspace interference

One of the primary issues with drones is interference in airspace being used by or designated for other traffic, resulting in what is effectively a denial of service attack for the airspace in question. A good example of this is the airspace around an airport, which is very busy and carefully managed by air traffic control systems and operators. Injecting a drone into the middle of this airspace would clearly cause a great number of problems, potentially even resulting in loss of life. Similar issues can be seen around various government installations, the scene of wildfires or other emergencies, and so on.

Presently, there is no good way to deal with such interference, although solutions are being developed to do so, as necessity is quickly bringing them into existence. We will return to this topic shortly.

Surveillance and privacy

Given the number of uses that drones are put to, issues around surveillance by drones and of the data produced by them are a large concern.

Clearly, there are a large number of concerns that revolve around the use of a flying platform equipped with a high definition camera and fully capable of recording images and video, whoever may be at the controls, whether police, paparazzi, or the neighbor next door. Scores of incidents involving snooping drones reported to the police,[2] being inappropriately used by police,[3] being shot out of the air by naked celebrities,[4] and a myriad of other such activities involving people using drones for what basically amounts to spying on other people.

Slightly upstream of this, there are also privacy issues surrounding the data that drones produce. In May 2019, the US Cybersecurity and Infrastructure Security Agency (CISA) accused Chinese drone manufacturer DJI of using data produced by its drones and sent back to its servers for intelligence use [7].

People behaving badly with drones

As a general catch-all category, potentially including both airspace interference and surveillance, there are seemingly

[2] Hannah Boland, “Police Say Drones Being Used to Vandalise Homes and Stalk Victims, As Reports of Incidents Surge,” The Telegraph (23 February 2019) – https://www.telegraph.co.uk/technology/2019/02/23/police-say-drones-used-vandalise-homes-stalk-victims-reports/.

[3] jprivate, “Police Use Drones to Spy on Suspicious People at ‘Potential Crime Scenes,‘ ” the Tenth Amendment Center (Apr 18, 2019) – https://blog.tenthamendmentcenter.com/2019/04/police-use-drones-to-spy-on-suspicious-people-at-potential-crime-scenes/.

[4] Andrea Park, “Mike Rowe of ‘Dirty Jobs’ Says He Pulled Shotgun on Drone Filming Him Naked,” CBS News (September 26, 2016) – https://www.cbsnews.com/news/mike-rowe-of-dirty-jobs-says-he-pulled-shotgun-on-drone-filming-him-naked/.

endless problems with drone-associated general bad behavior. Such events have included flying a drone without a license (a license is required in the US[5]), harassing wildlife, crashing drones into high-rise buildings[6] and a distressingly large number of other structures, and so on. Drone technology has now reached the price point and level of availability as to be available to the average miscreant.

Small-scale drone hacking

Security research and the Internet are full of tales of drone hacking. Drones use a variety of radio frequency (RF) signals, including regular Wi-Fi, to interface with the different portions of their flight control systems, receive updates, and other similar activities. This makes them easy targets for a variety of attacks including jamming to DoS them into a non-functional state or at least make them fly home and hostile takeovers of the remote systems being used to pilot them.

Tools for hacking drones are commonly available. A simple Internet search will turn up thousands of pages on the topic, with specific instructions available for a wide variety of commercially-produced devices.[7] Such efforts generally involve being in close range to the device in order to disrupt or hijack the signals being used to control or communicate with it.

Denial of service

Two of the primary tools that drones make use of for flight control, navigation, and communication are RF signals and GPS. Without these, the task of flying and navigating a drone would become considerably more difficult, if not impossible. As these are also very easy to disrupt, jamming or conducting a DoS attack can be as simple as directing interference at the drone on the same frequencies that its systems are attempting to make use of.

We can see a very public example of this in an incident from October 2018 during a drone-based light show that took place

[5] FAA, "Become a Drone Pilot," Federal Aviation Administration – https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot/.

[6] "Tourist Arrested after Drone Crashes into NYC High-Rise," US News & World Report (Oct. 22, 2018) – https://www.usnews.com/news/best-states/new-york/articles/2018-10-22/tourist-arrested-after-drone-crashes-into-nyc-high-rise.

[7] Sander Walters, "How Can Drones Be Hacked? The Updated List of Vulnerable Drones & Attack Tools," Medium.com (Oct 29, 2016) – https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809.

ISSA
EDUCATION FOUNDATION

News from the Foundation

The ISSA Education Foundation (ISSAEF) extended application deadline for the 2019 Foundation scholarships ended June 15, 2019. Applications from graduate and undergraduate students are currently being reviewed. Winners will be announced no later than August 2019.

A SUCCESSFUL MAY/JUNE for ISSAEF fundraising! At the ISSA Los Angeles' 11th Annual Information Security Summit, chairperson Sandra Lambert and ISSAEF director Lorraine Frost greeted visitors to ISSAEF's booth. ISSAEF director Deborah Peinert headed up the fundraising at the Denver Rocky Mountain Information Security Conference (RMISC).

Sandra Lambert and Lorraine Frost greeted conference attendees at ISSA LA's 11th Annual Information Security Summit.

Having a presence at two ISSA chapter conference events and the gracious support of individuals at the conference including many ISSA members resulted in nearly $2,000 to help fund future scholarships.

Serafino Sini donated his $100 winnings back to the Foundation.

The winners of ISSAEF's opportunity drawing were LA Chapter members Serafino Sini and Daryll Selga.

Smile when you shop at Amazon knowing 0.5 percent of your eligible purchases will be donated to our scholarship fund! Better yet, it won't cost you a dime. All you do is start your purchase from https://smile.amazon.com, select "ISSA Education and Research Foundation Inc." (one time). Don't forget to tell your family/friends to do the same.

Daryll Selga won the Smart Water bottle prize.

SEEKING VOLUNTEERS to participate in short-term projects, scholarship publicity, fundraising, and governance of the Foundation. Those interested in joining a truly dedicated and enthusiastic group, please contact Steve Haydostian at steve.haydostian@nbcuni.com or 818-777-8171.

Like us on Facebook and LinkedIn.

at the Hong Kong Wine and Dine Festival in Victoria, HK. The light show featuring 100 drones performing a choreographed display was attacked with a high-powered GPS jamming device. Of the 100 drones, 46 of them were disrupted to the extent that they fell into the water, despite having onboard safeguards that should have returned them to their point of takeoff. A reported HK$1 million in damages was caused by this attack [8].

Interfering with drone control systems

In a somewhat more complex type of drone attack than simple jamming, attackers can attempt to disrupt the signal from the ground control system or controller and take over in its place. This capability has been repeatedly demonstrated on different devices over the last several years and several security conference presentations have discussed the specific process involved.[8]

While such attacks aren't terribly difficult to carry out, nor do they require anything beyond off-the-shelf equipment, they are a one-drone-at-a-time effort. In order to carry out attacks on drones across a larger area, a considerable investment in infrastructure would be required.

Issues of scale

These types of attacks typically don't scale well. While we can, with relative ease, hijack a drone and control it or use a jamming device to render it unable to operate or force it down, this will typically be limited to at best a few drones in a limited geographic area. While we might be able to use this type of attack to harass or disrupt activities at a particular location, this doesn't quite satisfy the large-scale attack scenario that we're entertaining here.

Mirai in the Sky?

The interesting question, now that we've said that drone hacking and interference don't scale well, is how such attacks could be made to scale in the same way that botnet-forming malware attacks do. If this doesn't work well with a single drone or a small group of them in the same location, can it be made to work otherwise? Let's see...

What can we do with half a million devices?

Mirai, an IoT malware and associated botnet, reached its peak of over 600,000 infected devices in September 2016 [9]. Although a relatively simple and non-persistent malware, Mirai was able to use this set of infected devices (largely cheap IP cameras) to perform DDoS attacks on an at the time record-breaking scale of 1Tbps, a capability that was used to severely disrupt the services of large companies such as Amazon AWS and OVH.

If we posit a similar type of attack against drones on a large scale, the potential consequences could range from inconvenience to business disruption to loss of life. As an illustration of this, in December 2018 the London Gatwick airport suffered several days of air traffic disruption, believed to have been caused by only two drones. Nearly 1000 flights were diverted or canceled, impacting 140,0000 passengers over a period of three days [10]. Eventually not only was local law enforcement involved in the attempt to stop these attacks, but the British Royal Air Force was brought in as well. The attacks did stop after a few days, but not due to action on the part of law enforcement or the military.

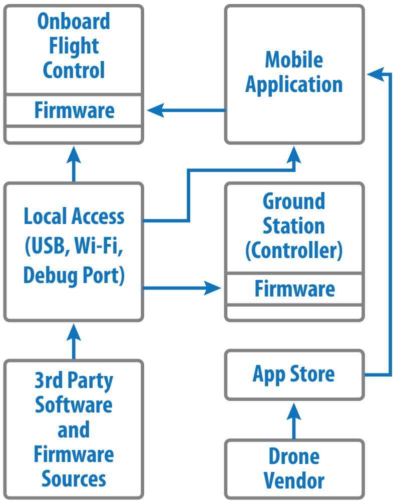
Onboard Flight Control
Firmware
Mobile Application
Local Access (USB, Wi-Fi, Debug Port)
Ground Station (Controller)
Firmware
3rd Party Software and Firmware Sources
App Store
Drone Vendor

Figure 2 - A drone flight control system

Given the very small scale of this attack and the asymmetrical impact that it caused, we can certainly see where anything on a larger scale than this would be absolutely paralyzing. Something along the lines of the half-million-device-strong level of the Mirai DDoS attacks carried out with drones may very well be beyond our present capabilities to cope with in any fashion.

Mass attack vectors for drones

We can easily see how something like this could happen with directly network-connected devices such as IP cameras, but how would this work with the somewhat distributed flight control systems that drones use? Let's take a quick look at a somewhat simplified block diagram for a common commercial or recreational drone, as is shown in figure 2.

The flight control system for this type of drone consists of three major portions: the onboard flight controller, an associated mobile application downloaded via the Android or iOS app store, and a ground station or controller. Firmware updates for the onboard flight computer are typically pushed from the associated mobile device application, and firmware for the controller is generally downloaded and pushed over USB from a computer.

Attacking drone firmware and mobile applications

In addition to the "approved" methods of updating drone applications and firmware, there are a number of very enthusiastic DIY communities and third-party commercial services. These sources provide entirely different tools and firmware, or hacked versions of official ones, that can be obtained on the Internet, which can be used to update various portions of the flight control system. Again, we can easily see the parallel here to the days of yore where shady third-party app stores existed for jailbroken mobile devices.

[8] Nils Rodday, "Hacking a Professional Drone," Black Hat Asis 2016 – https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf.

Such hacks are often performed to remove limitations put in place by the vendor such as restrictions on drone altitude ceiling, flight speed, no-fly zones around sensitive airspaces such as airports, and so on. Given a vector such as a commonly distributed hacked firmware, attackers might have a good way to gain a foothold in order to execute a mass hacking of drones.

Additionally, the mobile application portion of the flight control system provides a good avenue for attack. Mobile apps can be decompiled by attackers to find weaknesses or attacked from other applications installed on the mobile device—such security issues are all too common in the mobile app security space.

While we might like to think that it would take a certain amount of sophistication on the part of the attacker to rewrite drone firmware to carry out a complex set of malicious activities in order to fly into sensitive airspace and cause disruption, this really isn't the case. With the manufacturer caps on height and range removed, many common drones can easily reach thousands or tens of thousands of feet in altitude [11]. A relatively simple firmware hack that managed to reach even a few hundred drones across the country and directed them to rise to a few thousand feet on takeoff and stay there to the limit of their battery power would cause nationwide chaos. Executed carefully by an attacker to maximize the number of impacted devices, this could be devastating.

Attacking vendor backend systems

In addition to attacking the drone firmware or applications, the vendor backend systems might also provide an avenue for mass drone attacks. Introducing maliciously crafted firmware into the build pipeline of the manufacturer is certainly not outside the realm of possibility. The tactic of attacking software distribution systems in this manner is now time-proven, with large incidents over the years such as the BlackPOS malware attacks that impacted point of sale systems at retailers such as Target and Neiman Marcus in 2013[9] or the ShadowHammer malware that was pushed out to ASUS laptops using the company's own update servers[10] at the beginning of this year.

As an aid to this, leaks of source code and keys from drone manufacturers is not unknown, as was the case with drone manufacturer DJI in both the leak of drone source code and private keys for encrypting communication between the drones and backend servers in 2018 [12] and the very similar leak of private SSL keys among other data in 2017[13]. Between these two incidents, it would have been possible, in theory, to conduct a man-in-the-middle attack or gain access directly to the environment to insert malicious firmware.

Attacking large-scale drone control systems

As discussed earlier, interfering with drone control systems generally does not scale well. Although we could jam or DoS a group of drones in an area, hijacking a large number of drones would be considerably more difficult, except…

We briefly discussed Amazon's use of drones as a package delivery system. Although there are not a great many details publicly available at this point as to how this system would work at scale, we would have to presume an automated flight control system in order to manage the very large number of drones that we would someday expect Amazon to be operating.

Systems like this, although presumably heavy with safeguards against such, would likely provide one of the best opportunities for a Mirai-type incident involving drones. Amazon, with its geographically distributed operation and in-theory very large number of drones, could if subverted potentially shut down nearly every airport in a country at once by flying all nearby drones into the middle of the airspace used by passenger and cargo planes.

Fixing the problem

The solutions to solving this problem are largely technical in nature. While new legislation around the use of drones certainly may provide direction for their use and deterrents for their misuse, they do not provide any great deal of control over someone putting a drone in the air and putting it to malicious use.

Mitigating attacks on drone firmware and mobile applications

Many of the issues discussed that could potentially lead to a Mirai-like incident involving drones revolve around attackers being able to alter the firmware in the drone itself or associated portions of the ecosystem involved in the drone's flight control systems. Fortunately, these are problems for which reasonable security controls already exist.

Maliciously crafted drone firmware can often be installed on commercially available drones, either by simply uploading the modified firmware or by jailbreaking the drone to allow the modified firmware to be installed. In the last few years, major drone manufacturers have been putting protections in place to disallow such activity but still seem to be fighting a losing battle, as evidenced by the easily googled drone hacking sites available to the general public and easy to execute for anyone with even a quantum of technical skill.

These same sorts of issues were once commonplace with mobile device operating systems such as Apple iOS and Google Android but have become much more difficult as these vendors have continually increased the security controls in place. The same will eventually happen with drones, but it may yet be a few years before we see parity in the strength of security controls and anti-tamper mechanisms for drones and their associated applications.

[9] Brian Krebs, "These Guys Battled BlackPOS at a Retailer," Krebs on Security – https://krebsonsecurity.com/2014/02/these-guys-battled-blackpos-at-a-retailer/.

[10] GReAT and AMR, "Operation ShadowHammer: A High-Profile Supply Chain Attack," Kaspersky (April 23, 2019 – https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/.

In addition to this, there are also a few drone-specific security controls starting to see the light of day. One such still-theoretical mechanism would use the drone's accelerometers and gyroscopes to roughly double check the location information that the flight control system was receiving from the GPS in order to detect either of these systems being internally or externally tricked about their current location [14]. While such efforts are currently rudimentary, there are sure to get better with time.

Mitigating attacks on vendor backend systems

Some portion of the flight control system for many drones resides outside of the device itself in mobile applications, ground control systems, and backend systems. Each of these points of connection provides opportunities for attackers to find a foothold in the environment.

While drones are a newer technology, relatively speaking, the components and systems on which they are based are generally not. We can see many similar ecosystems in common use today that are secured against very similar attacks with tried and true controls. The distributed nature of drone flight control systems shares some similarities with the online systems used for banking, which are rife with mutual authentication, checksums, authorization checks for actions taken by mobile applications, and so on—all with the goal of stopping unauthorized activity.

The question of malware or maliciously crafted applications/components being inserted into a legitimate development pipeline can be a bit of a tricky issue to handle, as there are often a great number of moving parts in this process. A few beginning investigatory questions to ask along these lines are:

- Where does the software in the development tool chain come from and are we sure of its integrity?
- What third-party components/libraries/software are being used and how do we know that they are safe?
- Can the integrity of software builds be validated through the entire pipeline?
- Is there a process for handling incidents in this area?

The answers to these will, of course, vary from one organization to the next, as will the follow-on steps to be taken. These are, however, important questions to ask, from both the vendor and consumer side of things.

Mitigating attacks against large-scale drone control systems

Mitigating attacks against large-scale drone control systems is, at this point, a bit of a black box. These types of systems, outside of military and government, are not currently commonplace and are largely experimental in nature. While we can point at a few large systems being trialed, such as those at Amazon, these are proprietary and not yet in a place of being open to the general public for easy inspection by security professionals and security researchers.

As with most anything that we might choose as an example in the security world, the answer to mitigation here is likely to be the old saw—defense in depth. Of particular importance would be controls around some of the areas that we have discussed, such as software/firmware integrity protections, security of the development environment and pipeline, and security in general of any networked or ground-based portions of the FCS. As we see commonly in the retail industry with the PCI environments that contain and process cardholder data, segmentation of and controls around the data flowing in and out of the environment housing the ground-based portions of the FCS would be critical here.

When all else fails...

A new and exciting drone market segment being brought to life by drone-related incidents is the anti-drone countermeasure industry. In broad strokes, these types of tools provide some means of remote disabling drones, often with lasers or jamming, often coupled with a detection mechanism capable of detecting in-flight drones in the sky.

The remote disabling mechanisms for these types of countermeasures may consist of radar jamming, more useful for commercial or military drones,[11] RF jamming,[12] useful across a broad spectrum of targets, or laser systems,[13] useful for blinding or destroying drones entirely. In the case of the Gatwick airport example, nearly six million pounds were spent to install such a system [15].

In many cases, drones that have gone out of contact with their remote-control systems are programmed to return to their home or point of takeoff, but this also assumes that the drone is behaving in accordance with what the flight control system was originally intended to do in such events. If a swarm of hijacked drones with altered firmware encountered such a countermeasure device, the result could potentially be difficult to predict. As is often the case with security controls, these types of systems are sure to evolve over time.

Coming soon to a skyline near you

While we haven't yet seen a mass takeover of drones in the way of a Mirai-type attack, this seems to be fairly inevitable. These devices are highly-complex chains of hardware, firmware, mobile applications, and bacend systems with ample opportunity for exploitation by attackers.

Just as we have seen common IoT appliances start at a level of zero security and slowly be forced into putting controls in place due to constant and unrelenting attack, the same will probably end up being true of drones and their ecosystems. This is almost sure to be exacerbated by the impending mass drone delivery fleets being planned by Amazon and other vendors, a situation sure to present a tempting target to attackers, particularly those with advanced capabilities and resources for these types of attacks, as we might see in a nation-state backed group.

Mitigating Supply Chain Risk through Insider Threat Programs

Continued from page 9

- DNS blocklists and reputation services
- Deployment and configuration of active network defense solutions like honeypots, honey-files, and honey-accounts
- Behavior-based anti-malware endpoint solutions
- Segmentation/micro segmentation approaches

A well-designed insider threat program can be used to detect attacks arising from both malicious insiders as well as detect supply chain-related threats, thereby mitigating risk. Start by enumerating the breach scenarios likely to arise from the supply chain and making sure that your organization's insider threat program accounts for those. Make this process part of each vendor evaluation and revisit the exercise at least annually to catch emerging risks in the broader threat landscape. To be effective, organizations must combine the ability to detect such issues with action or risk being the subject of the next breach-related headline. Since alerts from these controls are of high-quality, security operations teams should prioritize their investigation and include both supply chain and insider-risk scenarios in the team's incident response plan and playbooks.

From manufacturers to customers, the whole of the supply chain is becoming increasingly interconnected. The security of that supply chain, however, is no stronger than that of its weakest participant. Supply chains are complex, often global, and are an area of increased security exposure as they begin to intersect with geopolitical concerns as well as hacker tactics, techniques, and procedures. An effective insider threat program creates the capability to identify potentially malicious activities inside the IT environment and works to minimize the impact resulting from abuse-of-trust scenarios common to both the supply chain and the user community. If such a program is not part of your security model currently, consider adding it to your strategic security road map.

About the Author

Mike Klepper, CISSP, CISM, AVSE, is an information security professional with over 26 years of experience working with clients in the technology, manufacturing, retail, and healthcare verticals. In his current role Mike leads a team that conducts application testing, penetration testing, and incident response. Mike can be reached at mklepperinfosec@gmail.com.

[11] "In the Spotlight," IAI – http://www.iai.co.il/Shared/UserControls/Print/PopUp.aspx?lang=en&docid=47062.

[12] Leonardo Company, "Finmeccanica – Selex ES Launches Falcon Shield Counter-UAV System," Leonardo Company (15 September 2015) – https://www.leonardocompany.com/en/press-release-detail/-/detail/falcon-shield-launch.

[13] "HEL on Wheels: Rheinmetall's High-Energy Laser Effectors Get Moving," Rheinmetall Defence – https://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/themen_im_fokus/rheinmetall_hel_live_fire/.

Are we really looking at a science-fiction novel plot future where fleets of hijacked drones are shot down by automated lasers and jamming systems over sensitive airspace? We would like to be able to say no to this, but several years ago who would have predicted tech giants being knocked off of the Internet en-masse by fleets of malware-controlled IP cameras. It is indeed a brave new world.

References

1. N. Kolakowski. 2013. “Amazon Drones Could Face Some Grief from FAA,” Dice – https://insights.dice.com/2013/12/02/amazon-drones-could-face-some-grief-from-faa/.
2. Amazon. 2016. “First Prime Air Delivery,” YouTube – https://www.youtube.com/watch?v=vNySOrI2Ny8.
3. J. Purkiss and J. Serle. 2017. “Afghanistan: Reported US Covert Actions 2017,” The Bureau of Investigative Journalism – https://www.thebureauinvestigates.com/drone-war/data/get-the-data-a-list-of-us-air-and-drone-strikes-afghanistan-2017.
4. S. Morrow. 2018. “Beware of the drone! Privacy and Security Issues with Drones.” Infosec Institute – https://resources.infosecinstitute.com/privacy-and-security-issues-with-drones/.
5. J. Feist. 2019. “Military Drones – the New Air Force,” DroneRush – https://www.dronerush.com/military-drones-air-force-navy-marines-cia-10853/.
6. FAA. 2019. “Recreational Flyers & Modeler Community-Based Organizations,” Federal Aviation Administration – https://www.faa.gov/uas/recreational_fliers/.
7. A. Villas-Boas. 2019. “The US Just Warned That Drones Made in China Could Be Used As a Way to Spy, But Not in the Way You Think,” Business Insider – https://www.businessinsider.com/us-government-warns-drones-from-china-pose-spying-risk-report-2019-5.
8. S. McCarthy, W. Zheng, and D. Tsang. 2018. “HK$1 Million in Damage Caused by GPS Jamming That Caused 46 Drones to Plummet during Hong Kong Show,” South China Morning Post – http://www.xinhuanet.com/english/2019-05/21/c_138077881.htm.
9. E. Bursztein. 2017. “Inside Mirai the Infamous IoT Botnet: A Retrospective Analysis,” Elie – https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/.
10. M. Evans. 2018. “Gatwick Airport Drone Chaos: Man, 47, and woman, 54, Arrested in Crawley - Latest Live News Updates,” The Telegraph News – https://www.telegraph.co.uk/news/2018/12/22/gatwick-airport-drone-chaos-man-woman-arrested-passengers-brace/.
11. S. Butler. 2019. “6 Drones That Can Reach High Altitude 2019,” DroneGuru – http://www.droneguru.net/best-high-altitude-drones/.
12. SecurityNewspaper. 2019. “Programmer Is Sent to Jail for Leaking Source Code of Chinese Dronemaker DJI,” Security Newspaper – https://www.securitynewspaper.com/2019/05/02/programmer-is-sent-to-jail-for-leaking-source-code-of-chinese-drone-maker-dji/.
13. G. Corfield. 2017. “Drone Maker DJI Left Its Private SSL, Firmware Keys Open to World+Dog on GitHub FOR YEARS,” The Register – https://www.theregister.co.uk/2017/11/16/dji_private_keys_left_github/.
14. Zhiwei Feng, Nan Guan, Mingsong Lv, Weichen Liu, Qingxu Deng, Xue Liu, and Wang Yi. 2017. “Efficient Drone Hijacking Detection Using Onboard Motion Sensors,” In Proceedings of the Conference on Design, Automation & Test in Europe (DATE ‘17). European Design and Automation Association, 3001 Leuven, Belgium, Belgium, 1418-1423.
15. BBC News. 2019. “Gatwick and Heathrow Buying Anti-Drone Equipment,” BBC News – https://www.bbc.co.uk/news/uk-46754489.

About the Authors

Clara Andress is an application security expert, with a strong background in development and operations. She is a recovering government contractor and enjoys wearing many and varied hats. She may be contacted at clara.a.andress@gmail.com.

Dr. Jason Andress is a seasoned security professional, security researcher, and technophile. He has been writing on security topics for over a decade, covering data security, network security, hardware security, penetration testing, and digital forensics, among others. He may be reached at jason.andress@gmail.com.