# UNHACKABLE DRONES: THE CHALLENGES OF SECURELY INTEGRATING UNMANNED AIRCRAFT INTO THE NATIONAL AIRSPACE

KYLE WESSON AND TODD HUMPHREYS

On August 2, 2010, a Navy helicopter entered the highly restricted airspace above Washington, D.C. without permission [1]. The event might have passed as unremarkable but for the fact that no-one was piloting the helicopter: as an unmanned aircraft, it carried no humans onboard, and—somehow—the vital communications link to its ground operators had been lost. The 1,429-kilogram MQ-8B Fire Scout flew entirely on its own for 30 minutes, blithely drifting through the airspace near nation's capital [2, 3].

Ground operators at Naval Air Station Patuxent River in Maryland eventually regained control of the craft and ordered it to return to base, later diagnosing the cause of the unintended excursion as a "software issue." But in fact more than one error had occurred: not only did the Fire Scout lose its communications link, it failed to execute its "return-to-base" lost-link protocol. So even as one Navy official put a good face on the incident by praising the reliability of the unmanned aircraft's autopilot system [3], most saw it as a disconcerting example of the unresolved safety and security issues surrounding unmanned aircraft.

The cost advantages of unmanned aircraft are compelling and will almost surely make these craft a component of everyday life in years to come. For the price of renting a human-piloted aircraft for a single power line inspection flight, a utility company could buy an entire unmanned aerial vehicle system to do the same job repeatedly. FedEx's CEO and founder, Fredrick W. Smith, has talked about using drones to replace the company's fleet of package-delivery aircraft [4]. For search and rescue, agriculture, infrastructure monitoring, research, and myriad other applications, unmanned aircraft—or drones in the common vernacular—provide convenience and economy. Recognizing this, the U.S. Congress passed the FAA Modernization and Reform Act in February 2012. The Act directs the FAA to draw up a "comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system" by 2015 setting the stage for broad drone use throughout the U.S.

But there is a growing public backlash. Having witnessed drones employed primarily for surveillance and missile strikes in conflict areas outside the U.S., many see no good reason to welcome them into the U.S. national airspace. Who will be piloting these craft anyhow? Where and why? And with no human pilot onboard looking out the window, won't they be more vulnerable to hijacking or hacking?

Echoing the concerns of their constituents, lawmakers in over 42 states have proposed drone legislation imposing limits on unmanned aircraft use. For example, Texas House Bill No. 912 would make it a misdemeanor for a drone operator to

*Date*: 1 April 2013.

capture images of private property from an unmanned aircraft without the property owner's "express consent"except under a set of narrow circumstances (e.g., law enforcement in pursuit of a suspected felon). At the federal level, the Preserving American Privacy Act of 2013 would prohibit law enforcement from conducting drone-based surveillance without a warrant and would outlaw armed drones by law enforcement or private citizens over the U.S.

## 1. A Sober Look at the FAA's Task

It is hard to imagine the FAA completing the task of drawing up a comprehensive unmanned aircraft integration plan by 2015 as required by the 2012 Modernization Act. Behind the FAA's standout safety record (witness the absence of fatal domestic aircraft incidents since 2010 [5]) is a slow-moving organization that reflexively associates innovation with risk. The FAA is already in the midst of a broad modernization called the Next Generation Air Transportation System, or NextGen, that will see satellite navigation replace radar as the primary sensor for air traffic control; the additional congressional demand to incorporate unmanned aircraft was no doubt unwelcome. In its 2012 report on the FAA's progress to-date on the Modernization Act, the Government Accountability Office concedes that the FAA has been handed a "daunting task" with an "aggressive time frame." [6].

Beyond the mundane logistical hurdles, integrating unmanned aircraft into the national airspace will also require the FAA to grapple with new security and privacy issues. The FAA's primary task is to ensure the safety of our public airways. Historically, this task was limited to preventing accidents due to human error or adverse natural conditions. After 9-11, it became obvious that a safe aircraft must also be secure against an attack by a scheming adversary; consequently, the FAA saw its role expand to include overseeing the installation of reinforced cockpit doors and crafting new security-conscious crew training procedures. From the FAA's point of view, aircraft security is now an integral part of airworthiness. This thinking logically extends to unmanned aircraft, bringing their security squarely within the FAA's purview.

As with security, the FAA has historically not been expected to grapple with issues of privacy related to aviation: it was left to the courts to decide whether someone in an aircraft had invaded someone else's privacy. But after the passage of the Modernization Act, the public is understandably concerned about the prospect of pervasive unmanned aircraft with high-definition cameras. Privacy advocates and members of Congress are now calling on the FAA to employ its regulatory authority to prevent breaches of privacy.

One might expect the Transportation Security Administration and its parent agency, the Department of Homeland Security (DHS), to take the lead in addressing unmanned aircraft security and privacy concerns. On paper, the Department of Transportation agrees, noting in its 2010 annual performance report that "[DHS] has primary responsibility for the security of the transportation system" [7]. But in practice, the FAA is unlikely to get much help from the DHS. In July 2012, Chairman Michael McCaul, speaking before a subcommittee hearing on "Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?", complained that "[DHS] officials repeatedly stated the Department does not see this function (domestic use of drones) as part of their mission and has no role in domestic unmanned aerial systems" [8].

The FAA appears resigned to shouldering the burden alone. Under questioning about drone security and privacy in a February 2013 House Committee on Science and Technology hearing, FAA representative Dr. Karlin Toner revealed that the Administration had formed a study group to examine security threats against drones and had taken the lead in soliciting advice from the public on questions of privacy. The DHS was conspicuous by its absence at the hearing and in the commentary.

In short, whether the FAA welcomes the changes or not, its regulatory role has expanded over the last decade to cover issues of aircraft security and can be expected to expand further over the next decade to cover issues of privacy.

## 2. Security Concerns

Leaving privacy matters to privacy experts, we offer here a clear-eyed assessment of the security challenges that the FAA will confront as it integrates unmanned aircraft into the national airspace.

Whereas traditional pilots control their aircraft from within, with hands on the yoke and eyes in the sky, unmanned aircraft pilots control their craft remotely, sometimes allowing them to fly autonomously (whether by accident or intent). Autonomous operation leaves drones uniquely dependent on their various radio links: the receive-only links to Global Positioning System (GPS) satellites, the two-way command-and-control link to the aircraft's remote pilot, and one or more links to other aircraft. Disruption or corruption of any one of these links can have serious consequences.

### 2.1. **Navigation.**

Almost all unmanned systems in the coming years will depend on civil satellite navigation systems like GPS for navigation. To be sure, the navigation sensor suite of a typical civil unmanned aircraft also includes inertial sensors (accelerometers and rate sensors), magnetometers, altimeters, and in some cases a camera. Even so, a GPS receiver is fundamental to the sensor suite because, unlike the other navigation sensors, it works in all weather conditions and does not drift.

Military GPS signals have long been encrypted to prevent counterfeiting and unauthorized use. Civil GPS signals, on the other hand, were designed as an open standard, unencrypted and freely-accessible to all [9]. These virtues have made civil GPS enormously popular, but the transparency and predictability of its signals give rise to a dangerous weakness: they can be counterfeited, or spoofed. In fact, civil GPS is the most popular unauthenticated protocol in the world.

The vulnerability of civil GPS to spoofing has serious implications for unmanned aircraft, as was illustrated by a dramatic remote drone hijacking at White Sands Missile Range in June 2012. The University of Texas at Austin Radionavigation Laboratory conducted the demonstration at the behest of the DHS. From a standoff range of half a mile, our spoofing device commandeered an 80 thousand dollar drone and forced it to plummet toward the desert floor [10].

How was this possible? Spoofing signals can be near-perfect forgeries of authentic GPS signals because (1) the civil GPS signal definition is publicly available, and (2) there are no security provisions, such as digital watermarking or encryption, to thwart counterfeiters [11]. In the White Sands experiment, the drone, unable to distinguish between the authentic GPS signals and the forged signals we were transmitting, ultimately decided to believe the forged signals. Once fooled, it began taking its position cues from our spoofing device. When these signals indicated

that the drone was rising vertically upward, the drone's autopilot system reacted by descending to "maintain altitude." The craft was only saved from crashing by a safety pilot who forced a manual override.

The spoofing threat is not new; it was well documented in a 2001 Department of Transportation report, known as the "Volpe Report" [12]. But policymakers and GPS manufactures largely ignored the report's warnings until very recently, perhaps reasoning that a spoofing attack was so unlikely as to not warrant attention. And while GPS researchers have proposed a variety of fixes since 2001, stubborn challenges remain [13]. Techniques that harden GPS signals with cryptographic watermarking are years away from implementation, and non-cryptographic defenses that could be implemented sooner must first prove their reliability in the dynamic signal environment in which drones operate.

Jamming is another concern for GPS-reliant drones. Near the earth's surface GPS signals are extraordinarily weak: they have no more flux density than light received from a 50 Watt bulb 22,000 kilometers away. As a result, their reception is easily disrupted, or jammed, by non-GPS radio-frequency noise in the GPS spectrum [14]. In fact, it is harder not to degrade GPS signals than otherwise: almost any modern electronic system (e.g., a laptop) will dump substantial noise power into a GPS receiver at close range.

Not surprisingly, intentional jamming can be much more targeted and powerful than unintentional jamming, with serious consequences for drones. In May 2012, operators lost control of a 150-kg South Korean Schiebel S-100 Camcopter, which finally crashed into its ground control station, killing an engineer and wounding two remote pilots [15]. A follow-up investigation revealed that North Korean GPS jamming directed into South Korea had precipitated a sequence of events (including erroneous pilot actions) that led to the crash.

As this jamming incident and the University of Texas spoofing demonstration make clear, secure navigation systems are vital for the safe integration of unmanned aircraft into our skies. These systems will need to be spoof- and jam-resistant, detecting and artfully adapting to a disruption of the fragile GPS signals. In case of prolonged interference, they will need a safe "GPS denied" protocol, such as landing nearby or returning to base.

2.2. **Sense and Avoid.** By the FAA's own estimate, more than 10,000 unmanned aircraft will fly the U.S. skyways by 2030. Needless to say, interaction between unmanned aircraft, and between manned and unmanned aircraft, had better be collision-free. Just as traditional pilots use visual and radar cues to sense the presence of other aircraft and avoid collisions, so unmanned systems must also have a sense-and-avoid capability. But the Government Accountability Office notes that, so far, "no suitable technology has been deployed that would provide unmanned aircraft with the capability to sense and avoid other aircraft and airborne objects" while also complying with current FAA regulations [6].

Sense-and-avoid is especially challenging for small drones because these cannot accommodate existing airborne radar systems, which are prohibitively bulky and power hungry. Visible-light and infrared cameras offer an attractive alternative: modern cameras are high resolution, inexpensive, low-power, and compact. Unfortunately, cameras can't be trusted to see through clouds.

Several experts have come to conclude that the only viable primary sense-and-avoid solution for small drones is Automatic Dependent Surveillance-Broadcast, or

ADS-B, a critical piece of technology from the FAA's NextGen air traffic system [16]. An ADS-B transponder broadcasts an aircraft's position and velocity every second and receives similar reports from nearby aircraft. By 2020, the FAA will require almost all aircraft to operate ADS-B transponders [17]. So long as all aircraft in a given neighborhood—manned and unmanned—dutifully broadcast their positions and velocities through their ADS-B transponders, the sense-and-avoid problem becomes a multi-agent path planning exercise for which there are many safe protocols.

However, like civil GPS, ADS-B has a serious Achilles's heel: its transmissions are unauthenticated and can thus be counterfeited. This omission stems from the fact that development of ADS-B took place in a time when security was a minor concern. No-one was expected to broadcast fake ADS-B signals because this had never happened before and it was hard to imagine what would motivate someone to spend the time and effort do so. Needless to say, such a naive assumption is out of place in the 21st century [18]. The cost and effort required to mount an ADS-B attack are now alarmingly low; researchers from the Air Force Institute of Technology showed in 2012 that a variety of "false injection" attacks can be readily coded on a commercial software-defined radio platform and launched from the ground or air with a cheap antenna [19]. Attacks could cause aircraft to believe a collision is imminent, flood the airspace with hundreds of false transmissions, or prevent reception of legitimate messages.

False ADS-B messages would be problematic for small drones. Whereas a pilot in a snowstorm may quickly verify with onboard radar that a false aircraft is not, in fact, sitting 100 yards ahead in the flight path, a small drone may have no effective secondary sense-and-avoid capability with which to make such a determination.

The FAA is working to address the problem of false ADS-B messages through multilateration, a technique for locating the source of a transmission by measuring its relative arrival time at multiple ground receivers. But reliable multilateration depends on a robust and precise time alternative to GPS, a cost-effective embodiment of which remains elusive [20]. The FAA remains nonetheless, reporting in a 2010 assessment that "using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today" [17]. To the dismay of security researchers, the Administration declined to explain how it had arrived at this summary dismissal of the problem, citing the sensitivity of its study.

2.3. **Command and Control.** Unmanned aircraft are controlled by a wireless tether, the so-called command and control radio link between the operator and the craft. This link enjoys much better intrinsic security than the GPS and ADS-B signals because it fits in the mold of standard wireless communications signals, for which secure protocols have been developed. Thus, while the command and control link is in theory vulnerable to eavesdropping or counterfeiting, industry-standard encryption, if employed, should prevent this.

Nonetheless, as for any radio-frequency link, jamming is a concern. Loss of the command-and-control link is referred to as a "lost link" event. Much like with the loss or corruption of GPS signals, no satisfactory solution to the lost link problem has emerged. Operators typically configure their drones with a lost link protocol (e.g., return to base if link lost for more than 30 seconds), but these protocols invariably assume an absolutely reliable navigation system, which, as has been argued, may be an unreasonable expectation. If GPS signals are, for whatever

reason, unavailable, and the command and control link is suddenly lost, what should a drone be programmed to do?

Another acute challenge related to the command and control link is the scarcity of protected radio spectrum. Owing to this scacity, many drone manufacturers currently resort to transmitting command and control signals in unprotected radio bands (e.g., the so-called industrial, scientific and medical bands), rendering unmanned aircraft susceptible to unintentional interference from the many electronic systems that already legally occupy these bands.

## 3. Discussion/Conclusion

The extent to which an attacker could exploit the vulnerabilities of unmanned aircraft depends somewhat on the regulations that will govern their operation. In crafting regulations, the FAA will be continually confronted with a safety/utility tradeoff. A requirement that licensed unmanned aircraft always be maintained within line-of-sight of their (not so remote) operators would be good for safety, but would render drones utterly useless for a great number of legitimate applications. Likewise, requiring continuous active piloting of unmanned aircraft via the command-and-control link, and not allowing a remote operator to command more than one aircraft at a time, may increase resilience in the face of unforeseen events, but would put "dull" back in the "dull, dirty, and dangerous" missions that drones promise to eliminate. Remote control begs for autonomy, and autonomy is the future of unmanned systems.

Perspective is important when considering the security of unmanned aircraft, as their vulnerabilities have either exact parallels or close analogs in the world of manned aircraft. Planes can be hijacked, pilots coerced, communications interrupted, luggage compromised. Yet we continue to fly, not because we're unaware of the risks, but because convenience trumps them.

Drones will seek from us the same concession.

## References

[1] E. Bumiller, "Navy drone violated washington airspace," *The New York Times*, August 26, 2010.

[2] N. Grumman, "MQ-8B Fire Scout: Vertical takeoff and landing tactical unmanned aerial vehicle system," 2012, http://www.northropgrumman.com/firescout.

[3] K. Quinn, "Fire Scout incident called 'learning experience'," *DefenseNews*, August 27, 2010.

[4] C. Anderson, "Fred Smith: FedEx wants UAVs," *DIY Drones*, February 12, 2009, http://diydrones.com/profiles/blogs/fred-smith-fedex-wants-uavs.

[5] J. Mouawad and C. Drew, "Airline industry at its safest since the dawn of the jet age," *The New York Times*, February 11, 2013.

[6] U.S. Government Accountability Office, "Unmanned Aircraft Systems: Measuring progress and addressing potential privacy concerns would facilitate integration into the national airspace system," GAO-12-981, September 18, 2012, http://www.gao.gov/products/GAO-12-981.

[7] U.S. Department of Transportation, "FY2010 DOT annual performance report," January 2010, http://www.dot.gov/mission/budget/fy2010-dot-annual-performance-report.

[8] M. McCaul, "DHS abandons oversight of unmanned aerial drones inside us," Press Release, July 18, 2012.

[9] GPS Directorate, "Systems engineering and integration Interface Specification IS-GPS-200G," 2012, http://www.gps.gov/technical/icwg/.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, 2013, under revision after favorable reviews.

[11] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.
[12] John A. Volpe National Transportation Systems Center, "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," 2001.
[13] K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing: Securing the future of PNT," *GPS World*, Jan. 2012.
[14] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphreys, "Know your enemy: Signal characteristics of civil GPS jammers," *Inside GNSS*, Jan. 2012.
[15] G. Mortimer, "Schiebel S-100 crash kills engineer in South Korea," *sUAS News*, 11 May 2012.
[16] Special Committee 186, "Minimum aviation system performance standards for Automatic Dependent Surveillance Broadcast (ADS-B)," 2002, RTCA DO-242A.
[17] Federal Aviation Administration, "14 CFR Part 91: Automatic Dependent Surveillance–Broadcast (ADS–B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Final Rule," Federal Register, May 28, 2010.
[18] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?" *IEEE Security and Privacy Magazine*, 2014, submitted for review.
[19] D. L. McCallie, "Exploring potential ADS-B vulnerabilities in the FAA's NextGen air transportation system," Master's thesis, Air Force Institute of Technology, 2011.
[20] M. Narins, M. Lombardi, P. Enge, B. Peterson, S. Lo, Y. H. Chen, and D. Akos, "The need for a robust precise time and frequency alternative to global navigation satellite systems," *Journal of Air Traffic Control*, vol. 55, no. 1, 2012.