Security Vulnerabilities in Unmanned Aircraft Systems

Maretta Morovitz [*]

December 15, 2015

Abstract

Unmanned Aircraft Systems (UAS) or drones, as they are known colloquially, have shifted from a futuristic possibility to an accessible existing technology. With military, business, and even recreational applications, drone usage has increased significantly in recent years. In the private sector, due to the growth of online tutorials, communities, and inexpensive parts, any individual can buy or build a drone at an affordable price. While this accessibility allows mainstream access to the technology, it poses a serious security threat to both the military and civilian spheres. News stories of drones flying through, and landing in, restricted and even prohibited airspace showcase the physical threat posed by drones. Compounded with this physical threat, are the software and GPS vulnerabilities all too often found in UAS technology. These vulnerabilities turn drones designed either for military or civilian use into flying weapons for surveillance and destruction. To date, the US government has no uniform policy on how to monitor the entire United States airspace for the presence of these drones, either recreational or military, or how to safely neutralize a detected threat. This paper will examine the vulnerabilities most commonly found in drones and discuss the research currently being done to secure these systems.

1 To the Community

Unmanned Aircraft Systems (UAS) have become an increasingly prevalent technology both in the military and civilian spheres. However, while this technology presents many benefits, there are significant security vulnerabilities that could result in loss of life, destruction of property, invasion of privacy, or, in the case of military UAS, a breach in classified information. For the military the consequences are clear. These are flying weapons. Loosing control of such technology could have devastating impact on US interests at home and abroad. In the civilian sphere, there are several levels of threats. First, is the threat of terrorism or other violent acts through the use of

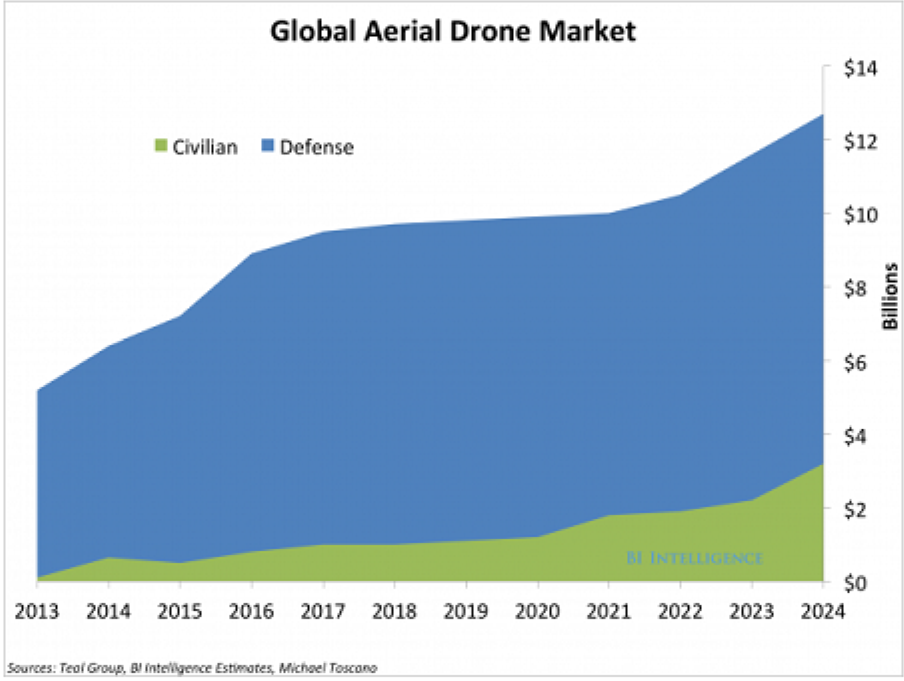
[*] Department of Computer Science, 161 College Ave, Tufts University, Medford, MA 02155. *email:* `maretta.morovitz@tufts.edu`

Mentor: Gabby Raymond

a weaponized UAS or reconnaissance UAS on US soil by a foreign agent. Second, is the threat of a friendly recreational drone being hijacked by unfriendly agents and used for malicious purposes. Finally, even friendly drones operated by friendly agents can cause problems if they fly through restricted airspace, such as the flight path of a commercial aircraft. While software vulnerabilities play little role in protecting against an armed UAS operated by a malicious agent, they can play a major role in allowing attackers to hijack friendly drones, or bypass security measures already in place to limit the available fly zones of recreational drones. Examples of attack methods include GPS spoofing and GPS jamming. Such attacks can alter the perceived location of the drone and either crash the system or allow the UAS to fly through restricted airspace. Additionally, malware such as Maldrone and SkyJack can hijack drones across multiple platforms, transferring control from the legitimate operator to the attacker. There are currently several ongoing research projects including DARPA's High-Assurance Cyber Military Systems (HACMS) program which, using formal methods, has produced the Secure Mathematically-Assured Composition of Control Models (SMACCM) Copter, which has been dubbed "the world's most secure drone" [21]. All of the SMACCMPilot software is available open-source to the hobbyist community. Additionally GPS alternatives are being researched through the DARPA All Source Positioning and Navigation (ASPN)project. Finally, a set of three ongoing programs called Patriot Sword, Shield, and Watch are designed to reduce the dependence of US systems on GPS signal, as well as detect and respond to intrusions to any US system receiving a GPS signal. Such research illustrates the importance of this issue to national security, as well as a way forward to a future where we can enjoy the benefits of UAS technology without the dangers that insecure UAS technology poses. UAS technology will inevitable become the way of the future, as the technology becomes increasingly accessible for military, commercial and private interests. As this happens, security must become a central priority. All drone manufactures, both commercial and private, must be cognizant of the security implication of their product. They must take the necessary steps to design secure software, or to use open source resources such as the SMACCMPilot. For the hobbyist community, education and awareness is key. Many of these individuals are unaware of the security vulnerabilities in popular commercial drones, as well as the need to build DIY drones from a security mindset. For the military, continued funding and support for projects such as HACMS, is the best way to ensure that the next generation of UAS is secure.

2 Context of the issue

In both military and civilian spheres, UAS usage has increased drastically in recent years. Military drone strikes, armed drone sorties, and missiles fired by drones have all nearly doubled in the past four years alone [15]. As can be seen Figure 1, both military and civilian drone markets are expected to continue increasing dramatically for the foreseeable future. In the civilian sector, the cost Ready-To-Fly (RTF) and Do-It-Yourself (DIY)drones have dropped significantly, ranging from $10s - $1,000s depending on the sophistication and size of the technology. These ranges allow drone enthusiasts, of every level, the opportunity to own and work with the technology.


Global Aerial Drone Market

Sources: Teal Group, BI Intelligence Estimates, Michael Toscano

Figure 1: Military and civilian drone markets have increased and are projected to continuing increasing dramatically [15]

Major companies such as Amazon have already announced future projects involving drone integration into their business practices. UAS are divided into two categories: military and civilian. Both sets experience similar types of vulnerabilities but with vastly different security and safety concerns and ramifications.

2.1 Military UAS The lack of an on-board human presence is one of the fundamental benefits of UAS, particularly in military use. No longer are American lives put in dangers as these drones fly over some of the world's most dangerous areas. Additionally reconnaissance drones are made much smaller than would be possible if an on-board human operator was necessary. However, while there are significant benefits to these computer operated systems, compared to legacy technology, UAS present a significantly increased risk of cyber-attack. On-ground operators rely on data, such as GPS positioning, to be transmitted back to operating bases. If these feeds are intercepted or modified, the operator may not even realize the data has been tampered with. Not only does intercepting this data represent a serious breach in classified information, but if the drone's piloting system is overridden by enemy combatants, the drones technology can be used against the United states. Or, as in the case of the Lockheed Martin RQ-170 model UAS captured in 2012 by the Iranian government, the drone can land in enemy hands without any defenses to protect sensitive information about the technology used to create and operate the UAS.

2.2 Civilian UAS Since civilian UAS are not typically carrying sensitive data or armed payloads, they often have little security in place, are easier to access, and are more prevalent in society compared to their military counterparts. This presents significant challenges, many of which have been the focus of recent media reports. Among these challenges are interference between drones and commercial airline, with over 650 sightings in the first half of 2015 alone.

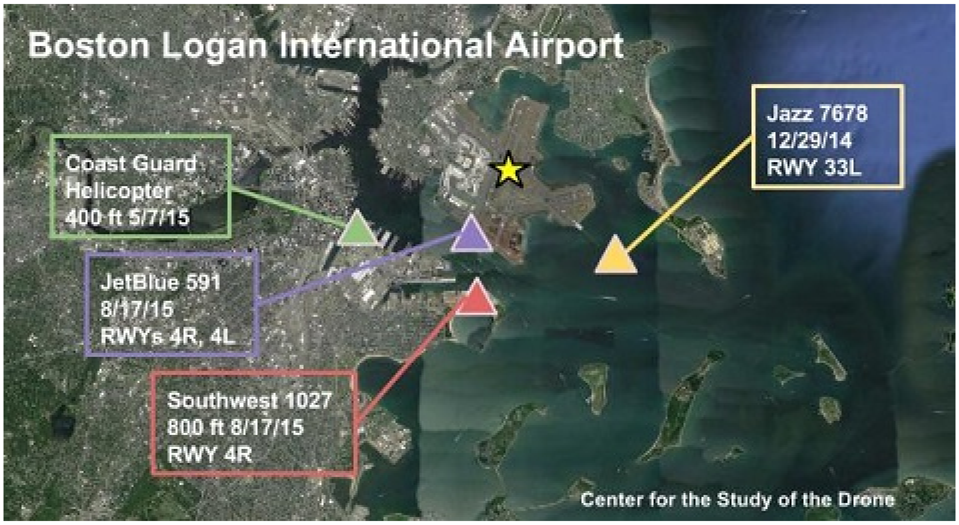

Boston Logan International Airport
Coast Guard Helicopter 400 ft 5/7/15
JetBlue 591 8/17/15 RWYs 4R, 4L
Southwest 1027 800 ft 8/17/15 RWY 4R
Jazz 7678 12/29/14 RWY 33L
Center for the Study of the Drone

Figure 2: Near miss incidents reported around Boston Logan International Airport

Civilian UAS are subject to flight restrictions around airports and recognized flight paths, however, uninformed operators mistakenly fly in these restricted zones. And, while the majority of these incidents are not malicious in nature, they pose two significant threats. Firstly, while no aircraft has been majorly damaged by a drone, the probability of a collision with resulting damage, injury or loss of life is high. Secondly, as previously stated, while the majority of these incidents are benign, there is no way to differentiate between a friendly and malicious drone from the air. Thus every incident must be approached cautiously. While drone and aircraft incidents are becoming increasingly frequent, they are not the only drone incidents reported in the media. In May of this year a drone crash landed on the White House lawn. While the drone itself did not pose a threat, it hints at a far greater danger. This particular drone flew through not just restricted, but prohibited airspace, and landed on the one of the most secure areas in our nation without interference. And while this UAS did not carry a dangerous payload, there is no guarantee that future UAS trying to access the White House will not. In another incident this year, a drone with traces of radioactive material landed on the roof of the Japanese prime minister Shinzo Abe's office as part of a protest of the country's nuclear energy policy. In both incidents no serious damage or loss of life occurred. However, these incidents should be considered a serious threat to national security. As a result of such incidents, many drone companies have begun implementing "geofences" to prevent future incidents. These geofences compare the drone's position to a blacklist of prohibited airspace, and prevent the drone from flying in such areas. However, as will be discussed later, GPS signal vulnerabilities present numerous ways for attackers to bypass such security measures. For many years, government research on counter-UAS technologies has focused on military usage. However, in light of recent threats, the government has begun the process of exploring counter-UAS technologies as applied to civilian usage. Most recently, MITRE, who operates a number of Federally Funded Research and Development Centers (FFRDC), has issued a nationwide challenge to "detect and safety interdict small UAS that pose a potential safety or security threat to urban areas". [17] Clearly, the presence of UAS in restricted airspace is a threat. But that is not the only danger with these systems. Before even considering civilian drones armed with dangerous payloads, a number of vulnerabilities exist both within the drones' software, as well as to the GPS signals used for positioning and navigation, that could lead to destruction of property, infringement of personal privacy, or even loss of human life. The following sections will explore the vulnerabilities that affect both military and civilian UAS, and the defenses currently available.

3 Vulnerabilities and Attack Methods

There are several categories of attack to which UAS are most vulnerable. Of these vulnerabilities, the majority are directly linked to some form of tampering with the UAS' on-board GPS system. A properly functioning UAS uses GPS to determine location and time, two critical pieces of data, especially in military operations.

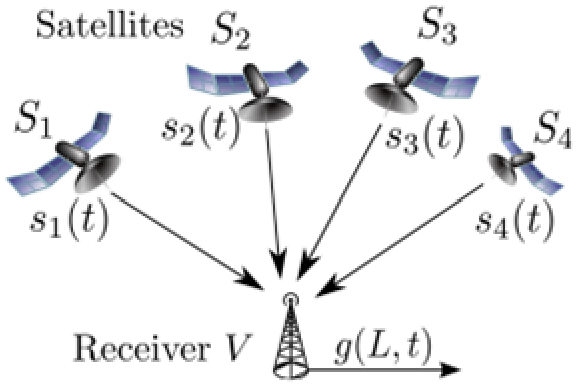


Figure 3: The UAS' GPS receives signals from a set of satellites and uses the signal delays [s_i(t)] to determine the position of the UAS and the time offset of the receiver V. [1]

This GPS signal is vulnerable to several types of attack including GPS spoofing and signal jamming attacks. While the methods may vary, the end result is the same: the UAS loses the valid GPS signal. For military UAS, this is a serious security breach as these systems contain sensitive and dangerous payloads. Incorrect or lost GPS signal can jeopardize the integrity and success of military operations. As previously discussed, while civilian UAS may not be equipped with weapons or other sensitive payloads, the do fly over a number of potential targets including civilian homes and communities, as well as have the potential to access high value locations. In addition to the threat of potential damage and loss of life, the ability to use civilian drones for reconnaissance is a threat to an individual's right to privacy. If the UAS' GPS signal can be altered, the attacker can bypass geofences and fly the UAS into prohibited airspace over civilian targets.

3.1 GPS Spoofing Generation Techniques At its core, a GPS spoofing attack relies on sending false GPS coordinates to a GPS receiver. The receiver then processes this fake data as real data, thus effectively masking the UAS' true location. In their paper entitled *GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques* A. Jafarnia-Jahromi, A. Broumandan, J.

Nielsen, and G. Lachapelle analyze the main types of GPS based attacks, the specific vulnerabilities that allow for these attacks, and potential countermeasures against these attacks [20].

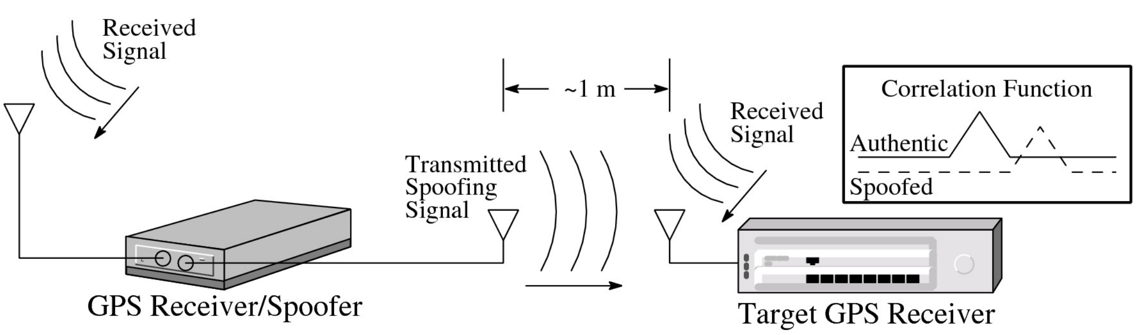


Figure 4: The attacker sends false data to the target's GPS receiver. The receiver processes this data and the target's GPS is falsified. [1]

GPS spoofing attacks differ based on whether or not the target is military or civilian. Civilian GPS uses unauthenticated GPS with unverified signals while military GPS uses authenticated GPS. In the case of civilian GPS, the attacker can delay or send premature signals, modify signals, or even generate new signals all without authentication. While military GPS uses authentication mechanisms to verify received signals, this does not mean that military UAS are entirely secure. Authenticated signals can be captured and resent to the receiver as valid signals. While this is a more complex attack, the end result is the same, the target receiver processes fake data as real. The operator no longer has valid information on the location of the UAS. Data such as time and date can be altered.

In addition to the differences in attack methods necessitated by civilian versus military GPS, there are three main categories of spoofing generation.

3.1.1 GPS Signal Simulator GPS signal simulators are designed to transmit a suite of realistic GPS signals [2]. Typically these simulators mimic realistic signal patterns that the target receiver often sees. However, since the receiver has no knowledge of the data being received by the target at any given moment, the attack data is often inconsistent and obvious to any human monitoring the received signal.

3.1.2 Receiver-Based Spoofers In a receiver-based spoofer, the signal spoofer is coupled with the target receiver. The spoofer first gains data to determine the target's current location, as well as synchronizes with incoming signals. Thus, unlike the previous category, these attacks do have knowledge of the target's current data, and thus can create more realistic and consistent attack signals. Generated signals can match actual signals in almost all areas, including geometric offset and signal strength.

While this type of spoofer is technically difficult, the hardware components are readily available and can be purchased for as little as a few hundred dollars. While this type of attack would be difficult to implement in a military setting due to highly restricted access to military devices, it poses a real threat to civilian UAS.

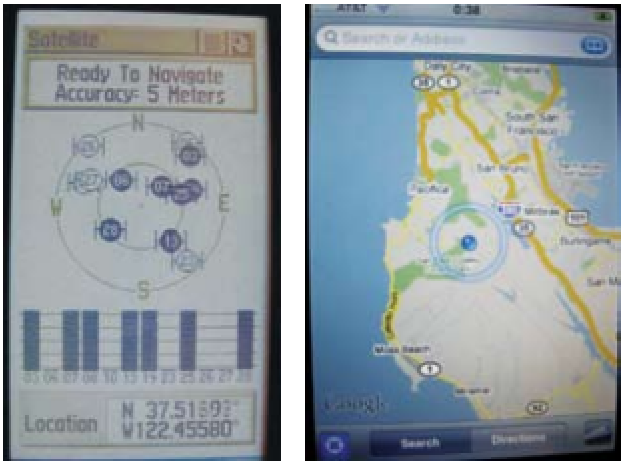


Figure 5: An example of a successful receiver-based spoofing attack on a commercial GPS receiver

3.1.3 Sophisticated Receiver-Based Spoofers This form of receiver-based spoofing is similar to the aforementioned attack, however unlike that attacked method, Sophisticated Receiver-Based Spoofers use multiple antennas. Additionally, the spoofer is capable of varying "the carrier and code phase outputs that are transmitted by each antenna and to control the relative code/carrier phases among these transmit antennas" [3]. While this attack is able to defeat direction of arrival anti-spoofing techniques, discussed in GPS Spoofing Counter Measures below, the attack is extremely technically difficult to perform.

3.2 Vulnerabilities to GPS Spoofing The vulnerability of GPS signals to spoofing can be divided into three categories, namely GPS vulnerabilities at the Signal Processing Level, at the Data Bit Level, and at the Navigation and Position Solution Level.

3.3 Signal Processing Level Vulnerabilities Many aspects of the GPS signal structure are publicly known including "modulation type, pseudo-random noise (PRN) signals, transmit frequency, signal bandwidth, Doppler range, and signal strength" [1] Additionally, GPS is a backward compatible technology, whose L1 frequency features are similar between generations of GPS satellites. Finally, commercial GPS uses automatic gain control (AGC) block to compensate for power fluctuation in signals, automatically adjusting the receiver input gain with the most powerful incoming signal. Thus the AGC increases the vulnerability of the receiver to attack as it adjusts to the spoofed signal. Knowing the structure and operation of a GPS receiver, the attacker can construct a realistic signal that will be accepted as valid.

3.4 Data Bit Level Vulnerabilities The framing structure of a GPS signal is publicly available. Additionally the navigation frame can be acquired quickly, but does not change rapidly. The attacker can take advantage of this signal stability and manipulate the GPS data frame. Finally, satellite health status bits can be manipulated, leading the receiver to reject valid signals.

3.5 Navigation and Position Solution Level Vulnerabilities Insertion of counterfeit pseudorange measurements by the attacker can lead to an incorrect position, velocity, and time solutions. This is key data and incorrect calculations effect vital UAS operations, especially in a military context

3.6 GPS signal jamming Another basic, but potentially destructive attack, is GPS signal jamming. While this attack lacks the subtlety of GPS signal spoofing, as the loss of signal is easily noticed, the result can be just as dangerous. Without a GPS signal, he UAS could lose the ability to monitor its route, location, altitude, and direction. Without these key pieces of data, the UAS may be rendered incapable of completing its mission. This is especially dangerous when a UAS is weaponized as part of a military operation. It can also pose a threat to civilian drone enthusiasts and, like the spoofing attack described previously, could allow UAS to fly past a geofence into restricted airspace if the geofences was not constructed to handle flying without GPS.

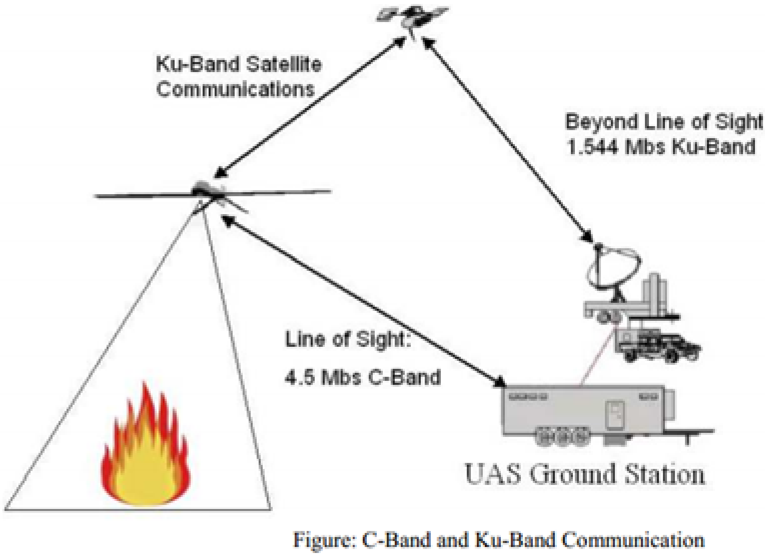

Ku-Band Satellite Communications
Beyond Line of Sight: 1.544 Mbs Ku-Band
Line of Sight: 4.5 Mbs C-Band
UAS Ground Station
Figure: C-Band and Ku-Band Communication

Figure 6: GPS signal jamming is a serious threat to UAS security

There is a wide abundance of GPS jammers available at low costs online. Even a simple Google search can result in a wide range of signal jammers available for as little as $20. This abundance and ease of access make this form of attack a major concern for drone security. And, while civilian GPS jammers may only have a short range, military grade jammers can cover 10s - 100s of kilometers. For example in 2010, it was discovered that North Korea had imported a truck-based GPS jammer capable of disrupting signals in a 100 kilometer radius.

3.7 Cyber-attacks malware based against UAS A final source of attack against UAS technology is via malware. Malicious code use has already infected military drones. In 2011, WIRED Magazine reported that a piece of malware infected US Predator and Reaper drones and recorded pilot's keystrokes during active war operations [9]. On the civilian side, two of the most popular pieces of malware are SkyJack and Maldrone. SkyJack is a UAS created by Samy Kamkar in 2013. The drone is designed to autonomously seek out, hack, and wirelessly take over other Parrot AR within wifi distance, ”creating an army of zombie drones under your control”. [10] The malware takes advantage of a backdoor in the wireless network. A second piece of malware known as Maldrone has proved that it is possible to, not only create malware to infect a particular drone, as done with SkyJack, but also create a piece of malware capable of infecting across different types of civilian drones. [11] Developed in 2015 by an India based security engineer named Rahul Sasi, Maldrone was first tested publicly on a Parrot AR drone. Sasi's malware was also successful on a DJI Phantom, a different civilian drone. The malware worked by targeting the drones drivers and sensors and then sending this information back to the attacker who could then use this data to control the drone. Creating an unhackable drone is currently an area of active research and will be discussed in the Research section to follow.

4 Defenses

4.1 GPS Spoofing Counter Measures There are a number of anti-spoofing methods commonly employed to detect spoofing attacks. The most basic is to use authenticated GPS, as in military drones. However, this type of signal is not used in the majority of civilian UAS. Additionally, as outlined previously, there are a number of attacks still possible even with authenticated GPS. Additional countermeasures to protect GPS signal integrity include: amplitude discrimination, Time-of-arrival discrimination, Consistency of navigation inertial measurement unit (IMU) cross-check, Polarization discrimination, Angle-of-arrival discrimination, Vestigial signal defense, and Jumps in space. [4] While these techniques exist, most recreational drones fail to implement such countermeasures.

4.1.1 Amplitude Discrimination Amplitude Discrimination analyzes jumps in amplitude, as well as the signal-to-noise ratio of the navigation signal for unusual or inconsistent behaviors. However, since receiver-based spoofing attacks can mimic signal amplitudes and strengths, this defense can be useless against such attacks. However, simple simulator attacks can be detected by this method.

4.1.2 Time-of-arrival discrimination Time-of-arrival discrimination searches for large clock offsets in a short time interval or sudden changes in phase signals. Both of these may be indicators of an unsynchronized attack. Again, receiver-based attacks are better at hiding from such methods of defense.

4.1.3 Consistency of Navigation Inertial Measurement Unit (IMU) Cross-check Consistency of navigation inertial measurement unit (IMU) cross-check uses a backup form or positioning to verify the detected GPS location. IMU uses a combination of accelerometers and gyroscopes, in addition to the initial coordinates to determine the current position. If the position calculated via IMU differs from the GPS determined position, a spoofing attack is detected. While this method is successful against most spoofing attacks, it is costly and complex to implement.

4.1.4 Polarization Discrimination Polarization discrimination verifies that received signals have the correct polarization. This countermeasure is successful only against unsophisticated attacks that send out spoofed signals with a different polarization than the original signal.

4.1.5 Angle-of-arrival discrimination Angle-of-arrival discrimination uses array antennas to check if the received signals are coming from the anticipated directions. Since valid signals are broadcast from various transmitters, the arriving signals have different angles-of-arrival. In contrast, a centrally located attacker will send all signals from a centralized location, thus giving each signal the same angle-of-arrival. As previously mentioned, sophisticated receiver-basted spoofing can get around this form of security, however that method is complex and difficult to apply in most situations.

4.1.6 Vestigial Signal Defense Vestigial Signal Defense relies on the fact that most attackers are unable to suppress the authentic GPS signal without access to the physical target receiver. Thus, the presence of a second, authentic signal is an indicator of a potential spoofing attack.

4.1.7 Jumps in Space A Jumps in Space method looks for unrealistic and impossible jumps in position. While this countermeasure is successful when an attacker suddenly changes the location of a UAS by several kilometers, more devious attacks may gradually introduce errors in the UAS location and thus avoid triggering a jump in space countermeasure.

4.2 GPS Jammer Countermeasures In the past, anti-jamming technology was large and extremely expensive. Recent advancements, such as the NovAtel Anti-jamming antenna currently undergoing testing by the Canadian armed forces for military applications, represent small light weight solutions to GPS jamming attacks. [23] Besides these burgeoning areas of anti-jamming research the only way to definitively avoid GPS jamming attacks, as well as all other GPS based attacks, is to rid UAS of their dependence on GPS signals. Three ongoing US programs sponsored by the Department of Homeland Security and Overlook Systems Technologies, Inc., a government contractor, called Patriot Watch, Patriot Shield, and Patriot Sword are designed as a "proposed solution to address risk to US critical infrastructure" relying on GPS services.[5] These programs were charge to

"...identify, locate, and attribute any interference within the United States that adversely affects use of the Global Positioning System and its augmentations for homeland security, civil, commercial, and scientific purposes." This three part program works to create a network of sensors to detect disruptions in US GPS services (Patriot Watch), defend US infrastructure dependent on GPS services (Patriot Shield), and an offensive strategy to provide a "measured and scalable response" [5] to prevent malicious usage of civil GPS in the US (Patriot Sword).

Another alternative to GPS, focused particular on UAS navigation was proposed by the DARPA All Source Positioning and Navigation (ASPN) project in 2013. According to DARPA, this project addresses the major threats against GPS though the following efforts:

1. Better inertial measurement units (IMUs) that require fewer external position fixes.

2. Alternate sources to GPS for those external position fixes.

3. New algorithms and architectures for rapidly re-configuring a navigation system with new and non-traditional sensors for a particular mission.

[8] An end-to-end system demonstration of ASPN was planned for Fiscal Year (FY) 15, however, to date, no information on this demonstration has been made publicly available.

5 Malware Counter Measures

One ongoing research program known as High-Assurance Cyber Military Systems (HACMS) is a DARPA based program that claims to have created the world's most secure drone. The project originated at the University of California, San Diego and the University of Washington. Kathleen Fisher is a Tufts Computer Science Professor and the original Program Manager of the DARPA HACMS program. Fisher explains that the HACMS software is "designed to make sure a hacker cannot take over control of a UAS. The software is mathematically proven to be invulnerable to large classes of attack [12] In an interview with Professor Fisher, she states that the drone running the HACMS software is the most secure drone in the world, even more secure than the drones currently flying in active military operations. HACMS was able to create this secure software through the use of Formal Methods (FM), a mathematical approach to software design. [13] According to Fisher, the use of FM can "eliminate many exploitable vulnerabilities" [21]. This is evidenced by the DARPA HACMS Program and the creation of the Secure Mathematically-Assured Composition of

Control Models (SMACC.

5.1 Formal Methods The DARPA HACMS program used formal methods to develop their secure drone software. As previously states, Formal Methods are a mathematical, machine-checkable application of ”theoretical computer science fundamentals...to problems in software and hardware specifications and verification.” [18] FM can be used for more than just identifying implementation bugs. FM can also identify faulty design, buggy specifications, side-channel information leaks, and dependence on third part software. While there are many benefits to using FM, there are also some trade offs. There is significant overhead in the lines of code required using FM. Additionally, while verified code is not necessarily slower, the process of verifying the code can be slow.

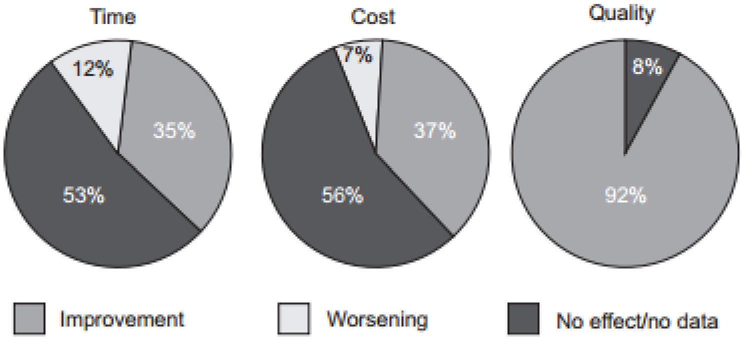


Figure 7: Effect of formal methods on time, cost an quality as determined in Formal Medthods: Practice and Experience [19]

The DARPA HACMS programmed used three different approaches to Formal Methods based systems: use of code synthesis, use of domain specific languages, and use of an interactive theorem prover. Specific examples of how the HACMS used FM to detect issues include: as a means to detect an unencrypted communication channels on the copter and to verify the functional correctness of the seL4 microkernel.

5.2 The HACMS Project As previously explained, the HACMS project used formal methods to create an unassailable UAS software for use in both the SMACCMCopter and the Boeing Unmanned Little Bird (ULB) Helicopter.

Program Setup	
Program Thesis	FM can yield UAS less susceptible to remote cyber-attack
Threat Model	No physical access, full knowledge of system and source code
Out-of-scope	Hardware assumed to be correct
Experimental Platforms	civilian quadcopter and Boeing Unmanned Little Bird (ULB)

Table 1: HACMS study setup

Figure 8: On the left is the Boeing Unmanned Little Bird. On the right is the SMACCM quadcopter using SMACCMPilot

The HACMS program structure was divided into 5 technical areas: vehicle experts, operating systems, control systems, research integration, and the red team. The vehicle experts were industry experts who understood the security vulnerabilities of UAS such as he Little Bird Unmanned Helicopter. The operating systems teams focuses on low-level architecture tasks. The control systems team focused on flight control system tasks. Research integration worked with the previous three technical areas to produce a working integrated high assurance system from high assurance components. Finally, the red team uses a formal methods based approached to penetration testing. The first four technical areas are present in two teams, the Air Team and the Vehicle team. The former, whose research this paper will focus on, worked on the Boeing Unmanned Little Bird

Helicopter and the SMACCMCopter.

In a baseline security assessment, the Red Team could take over control from both the AR drone quadcopter and ULB operators. The team used Aircrack-ng, an readily available package to "monitor and eject traffic onto wireless networks" [21]. First the red team identified the physical address of the drone's access point. The team then sent commands to deactivate the ground station. At this point, the red team had full control of the drone. However at the end of the first of three 18-month phases, the Red Team found no security flaws in 6 weeks with full access to the SMACCMCopter source code. Additionally the Air Team proved, through the use of FM, that the SMACCM system was memory safe, ignored malformed messages, ignored non-authenticated messages, and that all "good" messages received by the SMACCMCopter Controller reached the motor controller. This feat was achieved through several means.

5.3 Technical Area 4: Rockwell Collins Team The team responsible for technical area 4 was able to develop a formal architecture models for the SMACCMCopter and the ULB using Architecture Analysis and Design Language (AADL), a compositional verification tool called AGREE, an architecture-based assurance case tool called Resolute, and code synthesis tools. [21] These tools allow for properties about the system to be proved, and flagged automatically if the properties failed. For example, at the start of the project, the team built a high level description of the copter based on their current understanding. Later, as the team began to build that software, they used the actual system description. Their tools were able to automatically flag inconsistent properties. For example, in the simple model, the team had believed that there was only one way to communicate with the copter. However, this property was flagged as there was actually two ways to communicate with the copter. [21]

5.4 Technical Area 3: Galois Team The technical area 3 team was able to create embedded domain-specific languages (EDSL), called Ivory and Tower, while using Haskell as a macro language to put together the necessary C code. The team also built the SMACCMCopter using these languages. These languages allowed the team to synthesize flight-control code, models, and properties from one specification. Ivory is an open-source EDSL for synthesizing safe low-level code. This ensures that there are no common security vulnerabilities such as buffer overflows, null pointer dereferences, or memory leaks. Tower is a second open-source EDSL for describing specific tasks and how these tasks communicate with one another. These properties allow for low-level scheduling primitives to be hidden. Using approximately 10,000 lines of Ivory and Tower code, the team generated approximately 50,000 lines of C++ code which actually runs on the SMACCMCopter. Additionally, the Hardware Abstraction Layer (HAL), a part of the SMACCMPilot built by this team, is an open-source code that is currently available to the UAS hobbyist community. Finally, the team designed and built secure, open-source, and low bandwidth communication protocols. This system is also available to both industry, specifically Boeing, and the hobbyist community. [21]

5.5 Technical Area 2: NICTA The team from technical area 2 was able to formally verify full functional correctness of the seL4 microkernel. The team was able to prove "integrity, confidentiality, nontransitive interference, and intransitive noninterference" for the microkernel. [21] Additionally they used model checking to prove that the binary was directly implementing the C code in this specific compilation. They are currently in the process of conducting the same types of proofs for the eChronones RTOS. Finally they are working on synthesizing device drivers and file systems from high level specifications, as well as working on the CAmkES, a configuration language, which allows for the configuration of many other other pieces of the project.[21]

5.6 Technical Area 1: Boeing Boeing is working to integrate the work of the other HACMS technical areas into a high assurance version of the ULB. eChronos and the seL4 have been substituted on the Flight Control Computer and Vehicle Specific Module respectively. The team is currently on schedule to deliver a live flight demo of the ULB by the end of Phase 3 of the project. [21]

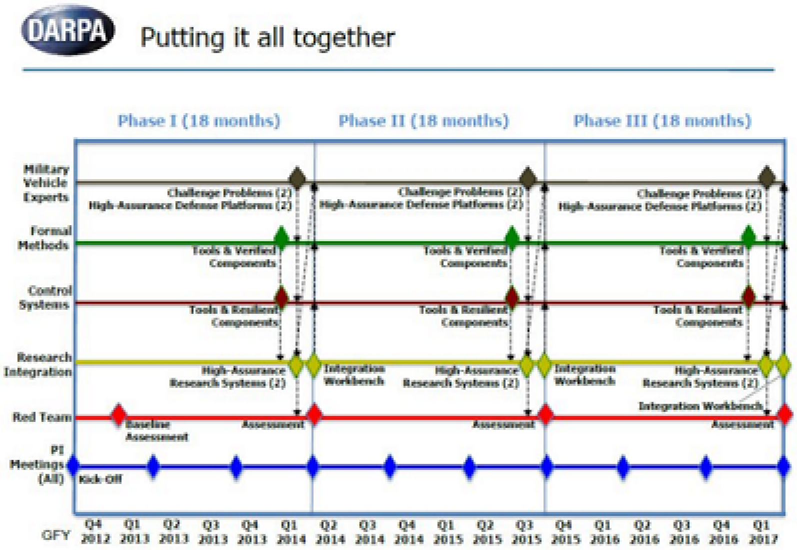

Putting it all together

Figure 9: The HACMS program was divided into 3 18-month phases each composed of 5 technical areas: TA1 Military Vehicle Experts, TA2 Formal Methods and Synthesis for OS Components, TA3 Formal Methods and Synthesis for Control Systems, TA4 Research Integration, TA5 Red Team [14]

6 The Future

UAS technology will inevitable become the way of the future, as the technology becomes increasingly accessible. As this happens, security must becomes a central priority as the technology develops and expands. As illustrated in the above report, current UAS technology is plagued with vulnerabilities, both related to the UAS software and its reliance on GPS signals. However, research through projects such as Patriot Shield, Sword, and Watch and the DARPA HACMS program represent significant steps towards creating safer more secure UAS technology. Additionally, MITRE's recent announcement of a nationwide UAS challenge showcases that the topic has moved to the forefront of the national security conversation. These conversations are essential if we, the security community, can hope to achieve more secure UAS technology. Additionally, the availability and promotion of software such as the SMACCMCopter software, to the hobbyist community is a necessary step to securing, not only military but also civilian UAS. Security education and awareness is key to promoting more secure hobbyist UAS.   UAS technology is the future, and could provide increased levels of technological integration both in our daily lives and in national defense. But steps must be taken now to ensure that we can enjoy the benefits of UAS technology and not be burdened by the disaster that could come from insecure UAS technology.

References

[1] ”Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Grard Lachapelle, GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, International Journal of Navigation and Observation, vol. 2012, Article ID 127072, 16 pages, 2012. doi:10.1155/2012/127072

[2]CCS ’12 Proceedings of the 19th ACM Conference on Computer and Communications Security, Raleigh (NC), USA, 16-18.10.2012. New York (NY): A.C.M., 2012. Web.

[3] Montgomery, Paul Y., Todd E. Humphreys, and Brent M. Ledvina. ”Azimuth Multi-Antenna SAR.” Multi-Antenna Synthetic Aperture Radar (2013): n. pag. Web.

[4] Becker, Georg T., and 2009 July 30. Security Mechanisms for Positioning Systems - Enhancing the Security of ELoran (n.d.): n. pag. Web.

[5] United States. Overlook Systems Technologies, Inc. Patriot Watch, Patriot Shield, Patriot Sword: A Proposed Solution to Address Risk to US Critical Infrastructure. By Inc. Overlook Systems Technologies. N.p.: n.p., n.d. Print.

[6] ”Patriot Watch - Patriot Shield - Patriot Sword.” Overlook Systems Technologies, Inc. N.p., n.d. Web. 15 Dec. 2015.

[7] GPS World Staff. ”Massive Jamming Attack By North Korea.” GPS World. GPS World, 8 May 2012. Web.

[8] Haas, Lin. ”Adaptable Navigation Systems (ANS).” Defense Advanced Research Projects Agency. DARPA, n.d. Web.

[9] Shachtman, Noah. ”Exclusive: Computer Virus Hits U.S. Drone Fleet.” Wired.com. Conde Nast Digital, 7 Oct. 2011. Web. 12 Dec. 2015.

[10] Kamkar, Samy. ”SkyJack.” Samy Kamkar. N.p., 2 Dec. 2013. Web. 12 Dec. 2015.

[11] Sasi, Rahul. ”Fb1h2s Aka Rahul Sasi’s Blog.” Garage4hackers Forum RSS. N.p., 26 Jan. 2015. Web. 12 Dec. 2015.

[12] ”Hack Proof Drones Possible with HACMS Technology.” General Security. InfoSec Institute, 3 June 2014. Web.

[13] ”Formal Methods.” Formal Methods Europe. N.p., n.d. Web.

[14] ”DARP HAMCS Program for Software Without Pervasive Vulnerabilities.” Security Affairs. N.p., 5 June 2014. Web.

[15] Woods, Chris, and Alice K. Ross. ”Revealed: US and Britain Launched 1,200 Drone Strikes in Recent Wars.” Drone Ware. All Stories, Covert Drone War, Drone Warfare, 4 Dec. 2012. Web.

[16] Insider, Business. ”THE DRONES REPORT: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications.” Business Insider. Business Insider, Inc, 27 May 2015. Web. 15 Dec. 2015.

[17] ”MITRE Challenge.” The MITRE Corporation. N.p., n.d. Web. 15 Dec. 2015.

[18] Understanding formal methods, jean-francois Mrtin 2003

[19] Woodcock, Jim, Peter Form Larsen, Juan Bicarregui, and John Fitzgerald. Formal Methods: Practice and Experience (n.d.): n. pag. Web.

[20] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Grard Lachapelle, GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, International Journal of Navigation and Observation, vol. 2012, Article ID 127072, 16 pages, 2012. doi:10.1155/2012/127072

[21] Fisher, Kathleen. ”ICFP 2014: Using Formal Methods to Enable More Secure Vehicles.” The International Conference on Functional Programming. Sweden, Gothenburg. 12 Dec. 2015. Lecture.

[22] Sasi, Rahul. ”Fb1h2s Aka Rahul Sasi’s Blog.” Garage4hackers Forum RSS. N.p., 26 Jan. 2015. Web. 12 Dec. 2015.

[23] GPS World Staff. ”Canadian Army to Test NovAtel GPS Anti-Jam Antenna.” GPS World. N.p., 06 July 2015. Web. 15 Dec. 2015.