Security Vulnerabilities in Unmanned Aircraft Systems

Maretta Morovitz, 2017[1];
Department of Computer Science, School of Engineering, Tufts University

Abstract

Unmanned Aircraft Systems (UAS), or drones. have become an increasingly prevalent technology both in the military and civilian spheres. 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. In addition to the obvious threat of a UAS operated by a malicious agent, more devious threats stem from vulnerabilities in GPS signals and malware backdoors that can allow attackers to hijack friendly drones, or bypass security measures in place to limit the available fly zones of recreational drones. There are several areas of active research to create more secure UAS with lessened dependency on GPS signal.

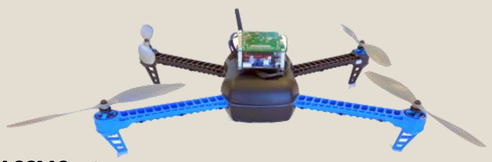

Figure 1: SMACCMCopter

GPS Spoofing Generation Techniques

In a GPS Spoofing attack, the attacker replaces the valid GPS signal with a counterfeit signal resembling the expected signal, or by rebroadcasting a valid, previously captured signal. [1]

1. **GPS Signal Simulator**: The signal simulator transmits a realistic unsynchronized signal pattern.
2. **Receiver-Based Spoofer**: The system synchronizes to the current GPS signals being received, extracting position, time, and satellite ephemeris. The spoofed signal is then generated with full knowledge of the 3D pointing vector of its transmit antenna toward the target receiver antenna.
3. **Sophisticated Receiver-Based Spoofer**: Similar to the aforementioned technique, but with the added complexity of utilizing several transmit antennas while simultaneously knowing enough data about the incoming signal to synchronize perfectly.

Malware

Military Malware Incidents: 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. [2]

Civilian Malware Incidents:

1. SkyJack: UAS created by Samy Kamkar. The drone finds and hijacks other Parrot AR drones using a backdoor in their wireless networks. The SkyJack pilot gains control of the drone, including all camera sources. [3]
2. Maldrone: Capable of infecting across different types of civilian drone platforms. Developed in 2015 by an India based security engineer named Rahul Sasi, Maldrone was first tested publically on a Parrot AR drone and then on a DJI Phantom. The malware targets the drone's drivers and sensors and then sends this information back to the attacker who could then use this data to control the drone. [4]

Current Research

DARPA's High-Assurance Cyber Military Systems (HACMS) program
Using formal methods, HACMS is designing and building the Secure Mathematically-Assured Composition of Control Models (SMACCM) Copter, which has been dubbed "the world's most secure drone" [5]. All of the SMACCMCopter software is available open-source to the hobbyist community. The HACMS software is also being implemented on the Boeing Unmanned Little Bird Helicopter. [6]

DARPA's All Source Positioning and Navigation (ASPN) project
DARPA is "developing sensors that 'use signals of opportunity' such as television, radio, cell towers, satellites, and even lightning, for real-time tracking". [7]

Patriot Sword, Patriot Shield, and Patriot Watch
This three part program is working to create a network of sensors to detect disruptions in US GPS services, defend US infrastructure dependent on GPS services, and an create an offensive strategy to provide a "measured and scalable response" to prevent malicious usage of civil GPS in the US. [8]

GPS Spoofing Vulnerabilities

The vulnerability of GPS signals to spoofing can be divided into three categories, namely GPS vulnerabilities in the: [1]

1. **Signal Processing Level**: The structure of a GPS signal is publicly available. Additionally, GPS is a backward compatible technology, whose L1 frequency features are similar between generations of GPS satellites. Finally, commercial GPS uses an automatic gain control (AGC) block to compensate for power fluctuation in signals, automatically adjusting the receiver input gain with the most powerful incoming signal.
2. **Data Bit Level**: The framing structure of a GPS signal is publicly available. Additionally the navigation frame can be acquired quickly, but does not change rapidly. Finally, satellite health status bits can be manipulated, leading the receiver to reject valid signals
3. **Navigation and Position Solution Level**: Insertion of counterfeit pseudorange measurements can lead to an incorrect position, velocity, and time solutions.

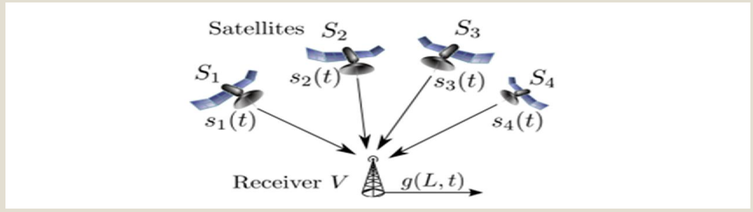

Figure 2: GPS signal

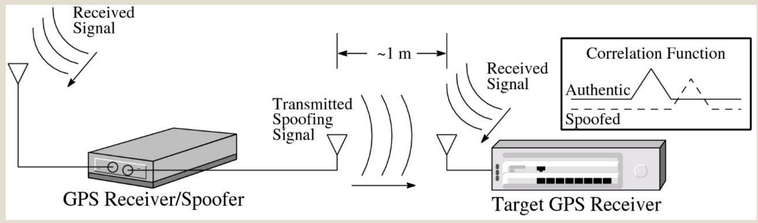

Figure 3: GPS Spoofing Attack

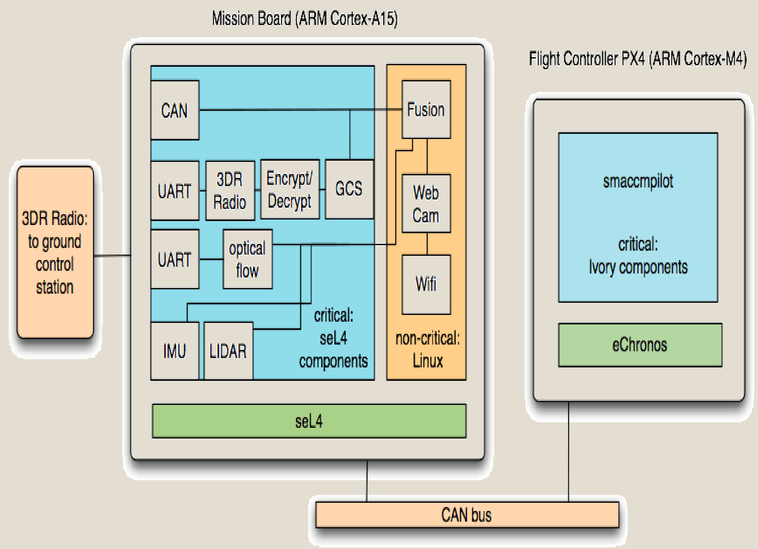

Figure 4: Block diagram of SMACCMCopter components

GPS Spoofing Countermeasures

There are a number of countermeasures designed to detect GPS spoofing attacks. Most involve examining specific aspects of an incoming signal for inconsistencies. [1]

1. **Amplitude Discrimination**: Detects jumps in amplitude and signal-to-noise ratio inconsistences.
2. **Time-of-arrival Discrimination**: Detects large clock offsets in short time periods or sudden changes in phase signal.
3. **Consistency of Navigational Inertial Measurement Unit (IMU) Cross-check**: Uses a backup form of positioning to verify GPS position.
4. **Polarization Discrimination**: Detects incorrect polarization in incoming signals.
5. **Angle-of-arrival Discrimination**: Compares the direction of incoming signals to anticipated directions. A normal GPS receiver receives signals from varying satellites at varying directions. This contrasts with a spoofed signal coming from a centrally located attacker.
6. **Vestigial Signal Defense**: Detects the presence of a second, valid signal.
7. **Jumps in Space**: Detects unrealistic or inconsistent jumps in position.

The Future

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.

Contact

Maretta Morovitz
Tufts University
Email: maretta.morovitz@tufts.edu
Website: mjmorovitz.github.io

References

1. "Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard 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. Shachtman, Noah. "Exclusive: Computer Virus Hits U.S. Drone Fleet."*Wired.com*. Conde Nast Digital, 7 Oct. 2011. Web. 12 Dec. 2015.
3. Kamkar, Samy. "SkyJack." *Samy Kamkar*. N.p., 2 Dec. 2013. Web. 12 Dec. 2015.
4. Sasi, Rahul. "Fb1h2s Aka Rahul Sasi's Blog." *Garage4hackers Forum RSS*. N.p., 26 Jan. 2015. Web. 12 Dec. 2015.
5. Fisher, Kathleen. Personal interview. 26 Oct. 2015.
6. Fisher, Kathleen. "ICFP 2014: Using Formal Methods to Enable More Secure Vehicles." The International Conference on Functional Programming. Sweden, Gothenburg. 12 Dec. 2015. Lecture.
7. Haas, Lin. "Adaptable Navigation Systems (ANS)." *DARPA RSS*. DARPA, n.d. Web. 12 Dec. 2015.
8. 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.