CERIAS

The Center for Education and Research in Information Assurance and Security

Analysis of Cyberattacks on UASs in Simulation

Scott Yantek, James Goppert, Nandagopal Sathyamoorthy, and Inseok Hwang

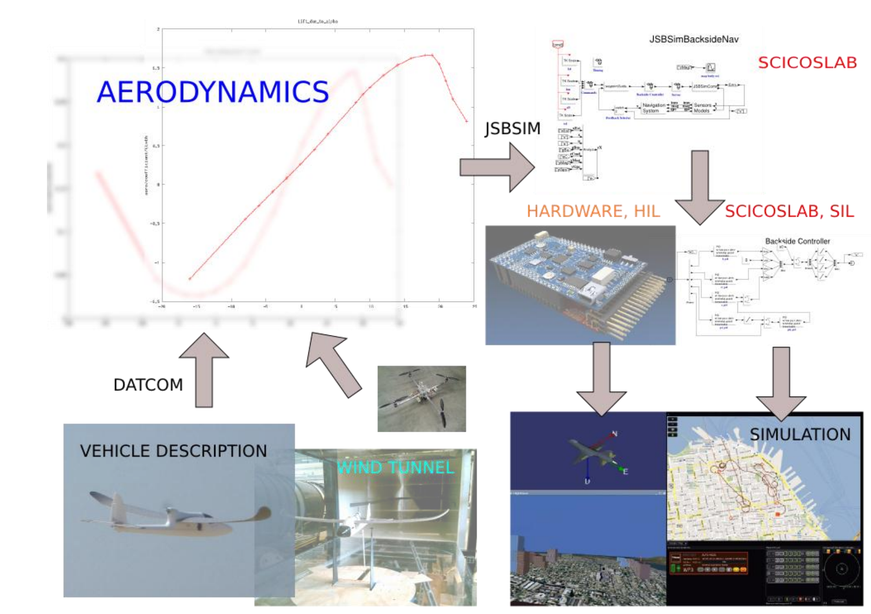
Abstract

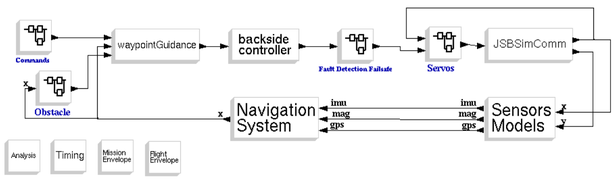
Unmanned aerial systems (UASs) have attained widespread use in military and research applications, and with recent court rulings their commercial use is rapidly expanding. Because of their dependence on computer systems, their high degree of autonomy, and the danger posed by a loss of vehicle control, it is critical that the proliferation of UASs be accompanied by a thorough analysis of their vulnerabilities to cyberattack. We approach the issue from a controls perspective, assuming the attacker has already gained some amount of control over the system. We then investigate vulnerabilities to certain types of attacks.

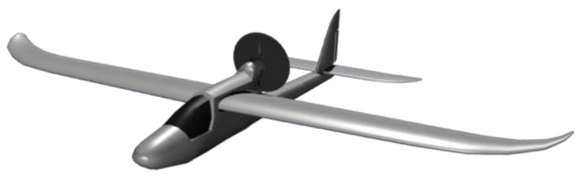
Simulation

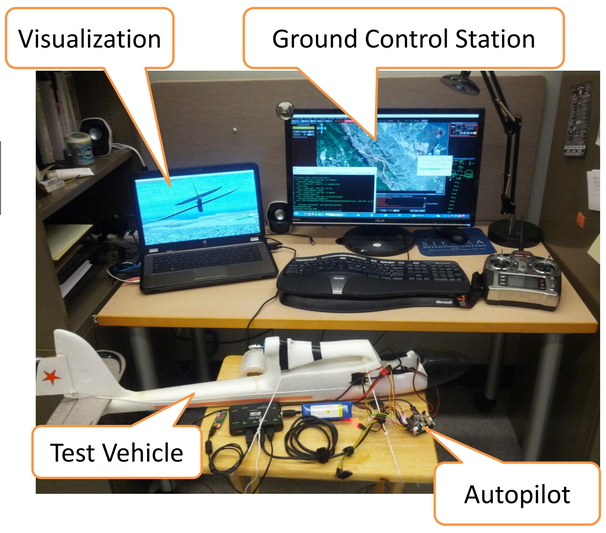
The Hybrid Systems Lab has created a simulation test bed that models UAS control systems and flight operations. This test bed is based on the open source PX4 autopilot and is capable of testing on both software-in-the-loop (SIL) and hardware-in-the-loop (HIL) levels. UAS flight can be simulated in the presence of various attacks, and attack success, severity, and detectability can be analyzed. The HIL simulation enables testing at both the design and implementation levels. When appropriate, attacks can also be tested on actual aircraft in flight.

Test Bed









Motivating Examples

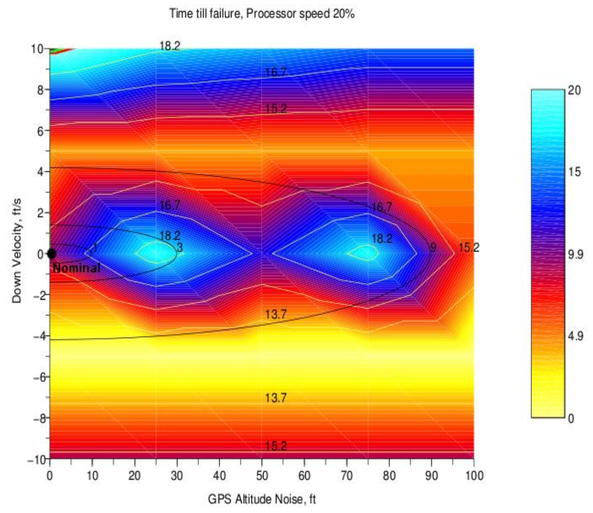
- The Stuxnet computer virus, discovered in 2010, caused Iranian centrifuges to spin out of control while at the same time resending old data showing normal function to the monitoring system.
- The US Air Force reported malware infections in UAS control system computers at Creech AFB in 2011. The infection was incidental and did not cause any reported damage, but demonstrates a vulnerability.

Attack Scenario

A malicious agent has gained access to the autopilot by exploiting a vulnerability (e.g. a buffer overflow) in the firmware. The vulnerability is either pre-existing, or it has been secretly inserted prior to the attack. The attacker uses knowledge of the system dynamics and architecture to use the vulnerability to carry out a stealthy attack.

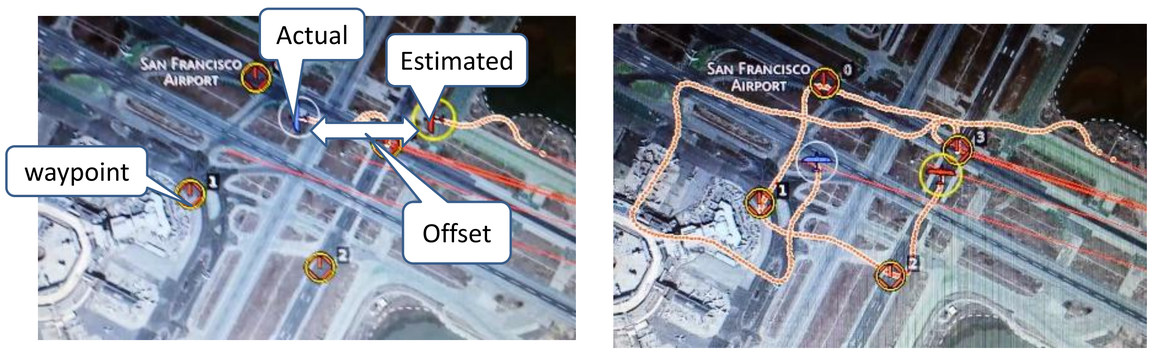
To identify possible attack strategies, we explored the effects of altering pairs of parameters, such as gains and noise levels, without any specific goals for the attack. We also consider an attack with the goal of driving the system to a state that is some desired amount away from the state intended by the operator, all without being detected.

Results



To the left is a plot of the time till failure for a combination GPS noise and velocity gain attack. The time till failure induced by this combination is one of the shortest out of all the simulations we ran.

Below are screenshots from a HIL simulation of a position offset attack, which adds a constant value to the measured longitude. This is a basic implementation of a more sophisticated attack, in which the position offset is slowly increased from zero to stealthily drive the UAS away from its goal to a different location where the attackers may then be able to land and capture it (at which point the attack is no longer stealthy). The particular scenario depicted below is not detected by the system because the offset is present from the beginning of operation, giving the autopilot no correct reference to compare with the bad data.



We would like to acknowledge Sypris Electronics for supporting this project.

CERIAS

PURDUE UNIVERSITY