SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework

Jiawei Yuan, University of Massachusetts Dartmouth; Houbing Song, Embry-Riddle Aeronautical University; Xiaolin Xu, Northeastern University

http://www.cis.umassd.edu/~jyuan/nsf_uav_security/index.html

The striking development of unmanned aerial vehicles (UAVs), or drones, is unleashing the increasing application in civilian and military scenarios. At the same time, serious cybersecurity concerns have been raised about UAVs, wherein they are identified as targets of cyber-attacks or potential attack vectors for malicious actors. This project seeks to improve UAV and cybersecurity education through the development of curriculum materials and hands-on laboratory platform.

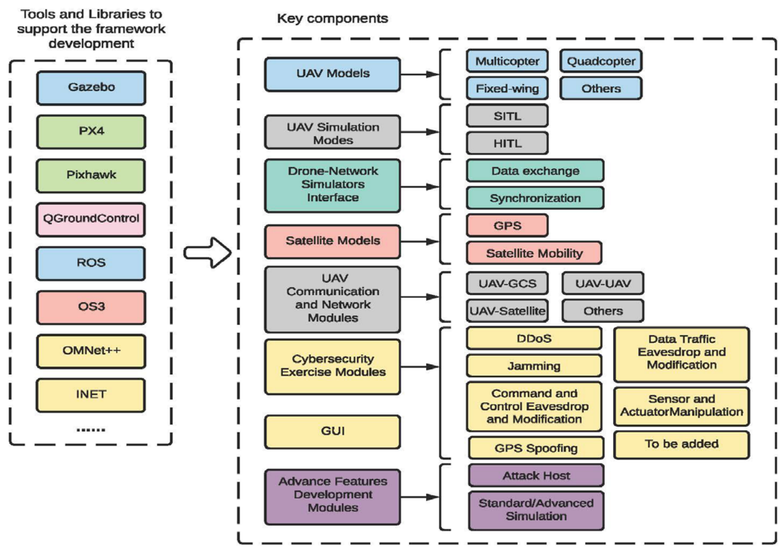
There still lacks curriculum materials on the cybersecurity of UAV. The education of UAV security is not simply composed of teaching separate UAV and cybersecurity topics but requires more analytic skills. Therefore, inadequate integration of UAV and cybersecurity courses without hands-on practice will be insufficient and ineffective. Besides, several other reasons make the development of UAV cybersecurity curriculum materials a challenging job.

1) Multi-disciplinary expertise is needed, such as UAV, avionics, computer science, hardware security, software security, network security, and cryptography.
2) The hands-on practice outcome (e.g., experiments) should be transferable and re-configurable at different institutions, especially at those with very limited UAV and cybersecurity facilities.
3) The development of curriculum materials, especially for hands-on components, must follow the FAA regulations and state laws.

As a conclusion, it becomes an urgent need to weave UAV into cybersecurity curriculum in a comprehensive way.

This project is the first to provide education materials, including hands-on labs on UAV cybersecurity systematically. The intellectual merit of the proposed project lies in its development of the novel, effective, and engaging course modules on UAV cybersecurity. The deliverables include a low-cost hardware-in-the-loop (HIL) UAV experimental kit; the integrated development environment (IDE) to use the tool kits; multiple hands-on labs covering the hardware security, communication security, network security, and data security.

This project seeks to improve UAV and cybersecurity education through the development of curriculum materials and hands-on laboratory platform. Specifically, this will include the development of 1) a set of cohesive course modules that systematically cover UAV cybersecurity topics; 2) a UAV cybersecurity laboratory platform that provides a series of exercise modules and can be easily deployed; 3) an open and collaborative UAV cybersecurity repository for educators, students, and researchers to discuss, collaborate, contribute, and share; and 4) faculty development summer workshops for UAV cybersecurity education.



The success of this project will produce the first systematic set of curriculum materials and hands-on laboratory platform for the education and training of UAV cybersecurity. From a long-term perspective, this will echo the increasing demand for high-skilled cybersecurity and UAV workforce from academy, industry, and military to meet national and economic priorities.

The proposed course materials will advance the education of UAV cybersecurity and general cybersecurity at multiple universities. Faculty from other universities may directly adopt the proposed curriculum materials in their courses.

The UAV cybersecurity education workshop will especially encourage the participation of faculty from minority-serving institutions or institutions with limited cybersecurity education resources.