Georgia Institute of Technology

ECE-8803: Cybersecurity of Drones Syllabus

Instructor Information

Saman Zonouz, Associate Professor
School of Cybersecurity and Privacy (SCP), and Electrical and Computer Engineering (ECE)
saman.zonouz@gatech.edu

General Course Information

Description

Cybersecurity of Drones is an in-depth exploration of security and privacy challenges in cyber-physical systems (CPS), with a primary focus on unmanned aerial vehicles (UAVs). This course equips learners with the foundational knowledge and hands-on skills necessary to analyze, attack, and defend drone systems in real-world scenarios. You will gain expertise in drone architecture, embedded systems security, adversarial machine learning, and CPS resilience, equipping you to understand and mitigate vulnerabilities in UAV operations. Through lectures, research paper discussions, and hands-on labs, you will engage with cutting-edge cybersecurity techniques, including sensor spoofing, actuator manipulation, malware analysis and defensive mechanisms tailored for autonomous aerial systems. By the end of the course, you will not only have a deep technical understanding of drone cybersecurity but also the ability to design resilient and secure UAV architectures, in preparation for careers in cyber-physical security, embedded systems, and critical infrastructure protection.

Pre- &/or Co-Requisites

- Basic Programming Proficiency (C/C++): You should have experience writing and debugging low-level code in C or C++, as drone systems often rely on embedded software and firmware.
- Computer Architecture and Embedded Systems: Understanding microcontrollers, real-time operating systems (RTOS), and assembly programming is essential for analyzing drone firmware and performing security assessments.

- Fundamentals of Cybersecurity: Prior coursework or experience in network security, cryptography, and ethical hacking will help you grasp UAV-specific cyber threats and defense strategies.

- Control Systems and Signal Processing (Recommended but not required): Knowledge of linear systems, feedback control, and sensor-actuator dynamics is beneficial for understanding drone flight control and cyber-physical attacks.

- Operating Systems and Reverse Engineering (Recommended but not required): Familiarity with Linux, system calls, and binary analysis tools will assist in debugging and securing UAV firmware and operating environments.

Course Goals and Learning Outcomes

By the end of the course, you will be able to:

1. Analyze the Security Architecture of Drone Systems: Evaluate the components and communication protocols of UAVs to identify potential cyber and physical vulnerabilities.

2. Demonstrate Attack Techniques Against Cyber-Physical Drone Systems: Implement and execute cyber-attacks, such as sensor spoofing, firmware exploitation, and control signal interception, to understand adversarial tactics and system weaknesses.

3. Design and Implement Security Mechanisms for UAVs: Develop and test secure architectures, intrusion detection systems, and cryptographic protections to enhance the resilience of drone operations.

4. Critically Evaluate Research in Drone Cybersecurity: Read, present, and critique cutting-edge research papers, articulating the strengths, weaknesses, and future research directions in UAV security.

5. Apply Cyber-Physical Security Principles to Real-World UAV Applications: Utilize industry-standard tools and methodologies to assess and improve the security posture of autonomous aerial systems, preparing for roles in critical infrastructure protection, defense, and cybersecurity research.

Course Materials

Course Text

For the Cybersecurity of Drones course, there is no single required textbook, but the following three books are recommended as supplemental reading material:

- Lee, Edward Ashford, and Sanjit Arunkumar Seshia. *Introduction to embedded systems: A cyber-physical systems approach*. MIT Press, 2017.

- Nise, Norman S. *Control systems engineering*. John Wiley & Sons, 2020.

- Sikorski, Michael, and Andrew Honig. *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press, 2012.

All supplemental reading materials are available in Canvas under the 'Reading List' tab.

Additional Materials/Resources

For the Cybersecurity of Drones course, you will need access to the following course technologies. This information will be provided in the Canvas course.

- Drone Simulation Platforms
  - ArduPilot (APM) / PX4: Open-source flight control software for UAV simulations and testing security vulnerabilities.
  - Gazebo / SITL (Software-In-The-Loop): Used for simulating drone behavior and cyber-physical attacks in a virtual environment.

- Embedded Systems and Reverse Engineering Tools
  - Ghidra / IDA Pro: For analyzing drone firmware and identifying security weaknesses.

- Wireless Security and SDR Tools
  - Wireshark: For network traffic monitoring and wireless security assessments.

- Programming and Development Environments
  - Python/C++: For developing drone security exploits and defense mechanisms.
  - Linux-based Virtual Machine (VMware / VirtualBox): Pre-configured with necessary cybersecurity tools for UAV research.

These technologies will be crucial for hands-on labs, penetration testing, security assessments, and developing drone security solutions throughout the course.

Course Website and Other Classroom Management Tools
The course will be hosted on Canvas.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignment Weight Distribution

Assignment	Weight
Paper Presentation (1)	20% • 10% presentation • 5% slides • 5% questions/comments/responses on others
Assignments (5)	30% • 1.5% Mini Project #1 • 7.5% Mini Project #2 • 7.5% Mini Project #3 • 7.5% Mini Project #4 • 6% Mini Project #5
Quizzes (16)	32%
Final Exam	18%

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A 90-100%
B 80-89%
C 70-79%
D 60-69%
F 0-59%

Description of Graded Components

i) Paper Presentations

Each student will select three research papers published in one of the four premier cybersecurity conferences — ACM CCS, IEEE S&P (conference), USENIX Security, or NDSS — within a single coherent UAV/CPS topic area. Students will prepare a 60-minute recorded presentation analyzing and critiquing each paper (10 minutes presentation + 5 minutes critique per paper), conduct a cross-paper technical comparison, and propose a novel research idea to address the same challenge. Deliverables include well-designed slides and a recorded talk. Evaluation emphasizes technical depth, clarity, analytical rigor, and engagement in peer discussions through constructive questions and responses on classmates' presentations.

ii) Quizzes

Sixteen online quizzes spaced across the modules to assess understanding of UAV architecture, control, embedded systems, and cybersecurity principles covered in lectures and readings. Each quiz contains a mix of conceptual and applied technical questions reflecting the week's learning outcomes, emphasizing physics-aware security reasoning and drone-specific attack–defense scenarios. Quizzes are open for a fixed window on Canvas and must be completed individually. They ensure continuous reinforcement of knowledge and preparation for the final exam.

iii) Final Exam
The cumulative final exam evaluates the student's integrated mastery of drone cybersecurity, control theory, embedded systems security, and CPS resilience. Questions require interpretation of control-loop models, attack vectors, and defensive mechanisms introduced throughout the course. The exam is proctored online and must be completed individually without external aids. It emphasizes synthesis of lectures, quizzes, and project material to test both conceptual insight and practical problem-solving ability.

iv) Mini Projects
Mini projects provide hands-on experience implementing and analyzing UAV cybersecurity concepts using simulation and firmware-level experimentation. Each project explores a distinct theme, such as MAVLink packet security, sensor-spoofing detection, control-loop anomaly analysis, or firmware vulnerability assessment, through Python/C++ coding and ArduPilot SITL simulation. Students will submit short technical reports and working code. Grading focuses on technical correctness, depth of experimentation, and the clarity of written documentation, encouraging creative application of course principles to realistic cyber-physical scenarios.

Submitting Assignments
All assignments (homework, knowledge checks, exams, etc.) must be completed and submitted within Canvas. Sending assignments (homework, knowledge checks, exams, etc.) directly to the professor, whether early, on time, or late, is not permitted and will not be accepted. If there are technical issues, please notify the Canvas help desk, as well as the professor, immediately. Canvas contact information is located under the "Communication Policy" below.

Assignment Due Dates
All assignments will be due at the times listed in the course schedule. These times are subject to change so please check Canvas announcements. Please convert from Eastern Time to your local time zone using a Time Zone Converter.

Late and Make-up Work Policy
No late assignments will be accepted. It's your responsibility to ensure a reliable internet connection for submission.

Grading and Feedback
All assignments, quizzes, and exams will be graded and returned with feedback within two weeks of submission. Feedback will be provided through Canvas. Students are responsible for reviewing their grades promptly after release and must submit any concerns or grade re-evaluation requests within one week of the grade posting date. After this period, grades will be considered final.

Technology Requirements and Skills

Computer Hardware and Software

- High-speed Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Windows for PC computers OR Mac iOS for Apple computers.
- Complete Microsoft Office Suite or comparable and ability to use Adobe PDF software (install, download, open and convert)
- Latest versions of Mozilla Firefox, Chrome and/or Safari browsers

Technology Skills

Students are expected to possess and apply a range of essential technology skills to be successful in this course. These include the ability to navigate a computer operating system (Windows, macOS, or Linux), install and launch applications, and manage files through downloading, saving, compressing (ZIP), and uploading to Canvas. Students should be comfortable using a web browser to conduct online research, connect to and troubleshoot Internet access, and send and respond to emails using professional communication etiquette. Basic proficiency with Microsoft Word and PowerPoint (or equivalent) is required for preparing reports and presentations. In addition, students must be able to operate a Linux-based virtual machine, execute Python and C/C++ programs, use command-line tools, and interact with UAV simulation platforms such as ArduPilot SITL, Gazebo, and Mission Planner. Familiarity with packet analysis tools (e.g., Wireshark), firmware analysis environments (e.g., Ghidra, IDA Pro), and version control (e.g., GitHub) is encouraged for completing hands-on drone cybersecurity assignments.

Onboarding Quiz and Proctoring Information

All Georgia Tech online degree and certificate students are required to complete the Onboarding Quiz with Honorlock in the first week of the course. Honorlock is utilized for student identity verification and to ensure academic integrity. Honorlock provides student identity verification via facial and ID photos. You may also be asked to scan the room around you. The Onboarding Quiz is needed to help make sure that your identity is verified and that your system is set up to work with Honorlock online proctoring tool. You are required to complete this quiz early in the semester to avoid problems when taking proctored exams.

Technology Help Guidelines

30-Minute Rule: When you encounter struggles with technology, give yourself 30 minutes to ‘figure it out.’ If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact Digital Learning Support at https://b.gatech.edu/digitallearningsupport.

When posting or sending email requesting help with technology issues, whether to Digital Learning Support, message board, or me, use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type “Help” into the subject field or leave it blank.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, always include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have already tried to remedy the issue (rebooting, trying a different browser, etc.).

Course Policies, Expectations & Guidelines

Communication Policy

- Email course questions and personal concerns, including grading questions, to me privately using saman.zonouz@gatech.edu. Do NOT submit posts of a personal nature to the discussion board unless it is a private post on Ed Discussions. On the other hand, please keep emails only for personal matters that cannot be shared on Ed Discussions; otherwise, all students should use Ed Discussions for their questions.
- Email will be checked at least twice per week on Mondays and Thursdays. During the week, I will respond to all emails within 3 days, excluding weekends and holidays. If there are special circumstances that will delay my response, I will make an announcement to the class.
- Ed discussion boards will be checked every other day by the TAs, excluding holidays and weekends.
- Virtual office hours will be held using Zoom. I will hold Virtual Office Hours every **Monday from 12:00 – 1:00 p.m. EST** (except 1/19 and 3/23), and **Thursday from 4:00 – 5:00 p.m**. **EST** (except 3/26), as well as special office hours for dedicated topics. Special topic hours will be announced in advance. I am also happy to schedule one-on-one office hours in person.
- For questions related to technology, the Digital Learning Support team at https://b.gatech.edu/digitallearningsupport for assistance. You can also reach the Canvas Hotline by phone at 1(877) 259-8498 or by email at support@instructure.com.

Online Student Conduct and (N)etiquette

Although it is not expected to be a problem in a graduate-level class, students are asked to behave in the discussions and other class interactions professionally and civilly. If you are in doubt, do not post it! Instructors reserve the right to remove any postings deemed inappropriate, unprofessional, or otherwise distracting from the course.

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If you choose to forward information to your university e-mail account, you are responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools, and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/policies/honor-code/.

Any student suspected of cheating or plagiarizing a quiz, exam, or assignment will be reported to the Office of Student Integrity, which will investigate the incident and identify the appropriate penalty for violations.

Collaboration & Group Work

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools, and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, see GT Honor Code website. Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, which will investigate the incident and identify the appropriate penalty for violations.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an

accommodations letter. Please also e-mail me as soon as possible to set up a time to discuss your learning needs.

Copyright
Among the materials that may be protected by copyright law are the lectures, notes, and other material presented in class or as part of the course. Always assume the materials presented by an instructor are protected by copyright unless the instructor has stated otherwise.

Student-Faculty Expectations Agreement
At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgment, and responsibility between faculty members and the student body. See https://catalog.gatech.edu/rules/21/ for an articulation of some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Subject to Change Statement
The syllabus and course schedule may be subject to change. Changes will be communicated via Canvas. It is your responsibility to check email messages and course announcements to stay current in your online courses.

Course Schedule

All times are Eastern Standard Time (EST/ET)

Course Activities		**Due Dates**
Module 1: Cyber-Physical Systems		
Lecture Videos		N/A
Quiz #1		January 18, 11:59pm
Module 2: Drone 101		
Lecture Videos		N/A
Quiz #2		January 18, 11:59pm
Module 3: Introduction to ArduPilot Autopilot		
Lecture Videos		N/A
Quiz #3		January 25, 11:59pm
Mini-Project #1		February 15, 11:59pm

Module 4: Drone Security - Overview		
Lecture Videos		N/A
Quiz #4		February 1, 11:59 pm
Module 5: Physics-informed Cybersecurity		
Lecture Videos		N/A
Quiz #5		February 8, 11:59 pm
Module 6: Drone Sensors		
Lecture Videos		N/A
Quiz #6		February 15, 11:59pm
Mini Project #2		March 1, 11:59pm
Module 7: Trustworthy AI-enabled and Conventional Perception		
Lecture Videos		N/A
Quiz #7		February 22, 11:59pm
Module 8: Drone Coordinate Frames		
Lecture Videos		N/A
Quiz #8		March 1, 11:59pm
Paper Presentation		March 22, 11:59pm
Module 9: Kalman Filtering		
Lecture Videos		N/A
Quiz #9		March 8, 11:59pm
Mini Project #3		March 29, 11:59pm
Module 10: Drone Dynamics		
Lecture Videos		N/A
Quiz #10		March 15, 11:59pm
Module 11: Drone Control		
Lecture Videos		N/A
Quiz #11		March 22, 11:59pm

Module 12: Firmware Security		
Lecture Videos		N/A
Quiz #12		April 5, 11:59pm
Mini Project #4		April 12, 11:59pm
Module 13: Communication Protocols		
Lecture Videos		N/A
Quiz #13		April 5, 11:59pm
Module 14: Cybersecurity-Informed Control		
Lecture Videos		N/A
Quiz #14		April 12, 11:59pm
Mini Project #5		April 27, 11:59pm
Module 15: Formal Security Verification		
Lecture Videos		N/A
Quiz #15		April 19, 11:59pm
Module 16: Putting It All Together		
Lecture Videos		N/A
Quiz #16		April 26, 11:59pm