Cybersecurity of Drones - Spring 2023

Class Time/Location:
Tuesdays and Thursdays
9:30-10:45 am
@ Van Leer C341

Instructor:
Prof. Saman Zonouz
saman.zonouz@gatech.edu
Coda E1062B

Office Hours:
Tuesdays 11am-12pm

About This Course

The course covers introductory topics in the security and privacy of cyber-physical systems especially unmanned aerial vehicles (UAVs) or drones. The goal is to expose students to fundamental security primitives specific to drones and to apply them to a broad range of current and future cyber-physical security challenges. Much of the course is taught with a focus on one instance of cyber-physical systems - drones. However, students will be expected to generalize the concepts to other cyber-physical systems.

Students will work with various hands-on tools and fundamental techniques used by hackers to compromise controllers and computing systems or otherwise interfere with normal cyber-physical operations such as a drone flight. Students will also use tools that are unique to interacting with cyber-physical systems. The purpose of the class is NOT to teach you how to be a hacker, but rather to teach you the approaches used by hackers so you can better defend against them. Students will be graded based on exams and the completion of assignments.

Course Goals and Learning Outcomes

After successfully completing this course, students should be able to:

1. Develop the ability to interact with cyber-physical drone systems components
2. Develop the ability to conduct attacks on cyber-physical drone systems
3. Develop the ability to design cyber-physical drone systems and architectures that are resilient to attack

4. Read and present cutting-edge research publications relating to security and privacy challenges in cyber-physical drone systems
5. Implement and test attacks and defenses in common cyber-physical drone controllers

Textbooks: None. Instead, we will study published research papers from top-tier academic venues in cyber-physical systems security. We will use a slide show to keep track of the papers we read in this class. Each paper will get slides that cover: “What problem is the paper focused on?”, “What solutions/techniques are proposed?”, “How did they evaluate their work?”, and “What future research opportunities can you think of?” These slides will be turned in for a grade at the end of the semester.

Pre- &/or Co-Requisites

ECE2035 or ECE2036 or CS2110 equivalent. Background knowledge in assembly and reverse engineering will be helpful and programming experience in C/C++ is a must.

Class Session Organization

The sessions will include mostly lectures on the fundamental concepts, research paper presentations, video demonstrations of the concepts, followed by hands-on tutorial sessions on drones. In-person class participation is highly recommended.

Homework assignments

The homeworks will be assigned on specified dates. All submissions will be online (no email submissions will be accepted). Each homework will have a submission deadline. Late submissions will not be accepted. It is the student’s responsibility to find a good quality network connection for the submission.

Research paper presentation

The students will be assigned to read and present recent top research papers on cyber-physical systems security in class. The presentation quality will be assessed based on the student’s understanding of the paper’s ideas, experimentations, weaknesses and strengths, and potential future work.

Reading Slides

Each week’s lesson is accompanied by published research papers from the top-tier academic venues in cyber-physical systems security. Please read these research papers as pre-readings to prepare for each class. Each student will use a slide show to keep track of these papers as they read them. Each paper must get at least 1 slide, and the slides must cover the following for each paper: “What problem is the paper focused on?”, “What solutions/techniques are proposed?”, “How did they evaluate their work?”, and “What future research opportunities can you think of?” These slides will be turned in for a grade at the end of the semester. Please keep it simple! 1 or 2 sentences for each question is sufficient. The grade is based on having a slide for all the papers and your understanding of each paper.

Grades and Feedback Request
Once grades for an assignment/exam/etc. are out, students may have complaints about the grades until one week after the grades’ release date - no more objections after one week will be accepted.

Exams
There will be one midterm exam and a final exam in the semester.

Semester-long Research Project (graduate students only)
The graduate students will have to complete a semester-long research project that will include all the steps required for a typical research paper publication on a smaller scale to fit within a single semester. These steps will include literature review, problem statement, solution idea and design, implementation, experimentation and validation, and final full paper writing. Each step will have a milestone and submission deadline associated with it.

Grading Policy:
Grades will be tentatively based on a point total computed as the following:

- Breakdown
    - Undergraduate:
        - 15% paper presentation + 10% reading slides + 35% homeworks + 20% Midterm exam + 20% Final exam
    - Graduate:
        - 15% paper presentation + 10% reading slides + 20% homeworks + 15% Midterm exam + 15% Final exam + 25% research project
- Gradelines:
    - The following gradelines will be used for the course:
      A [90, 100] - inclusive bracket;
      B [80, 90) - exclusive parenthesis;
      C [70, 80);
      D [60, 70);
      F [0, 60)

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, 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.

Copyright

The course readings include research papers that are available in the public domain or via the Georgia Tech library. As specified by publishers' copyright notices, the papers will be for individual use only. Similarly, course materials such as quiz and exam questions are for your use only and should not be published or disseminated.

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 the website, 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 in order to set up a time to discuss your learning needs.

Class Attendance

Class attendance is mandatory, and past experience have shown that students who are actively involved in class discussions have the best experience conquering this challenging subject matter. Course deadlines and assignments can be modified for students with documented absences. These accommodations must be arranged in advance and in accordance with the Georgia Tech Attendance Policy. More information about the institute's absent policy can be found here.

Topics we will cover in this semester will include:

- Introduction to cyber-physical systems
- Drones architecture and Ardupilot platform
- Introduction to sensors and actuators
- Embedded real-time scheduling
- Drone linear time-invariant models
- Attacks
  - Real-world malware on cyber-physical systems (e.g., Stuxnet, Triton, Blackenergy)

    - Sensor false data injection attacks
      (e.g., model-based techniques and adversarial machine learning)
    - Actuator control channel attacks and physics-aware malware
    - Value-agnostic timing attacks
- Defense
    - Prevention: formal methods and model-based verification
    - Detection (online): bad-data detection and controller software defenses
    - Response: AI-based controller surrogate, correct sensor value restoration, control-theoretic flight operation recovery
- Emerging artificial intelligence techniques in drone perception and control

Research papers

The following research papers are examples that will be discussed in the semester:

Paper title	Conference	Year	Link
SoK: Security and Privacy in the Age of Commercial Drones	IEEE S&P	2021	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9519393
Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors	USENIX Sec	2018	https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-tu.pdf
Flight Recovery of MAVs with Compromised IMU	IROS	2019	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8968145
WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks	IEEE S&P	2017	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7961948
Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing	USENIX Sec	2020	https://www.usenix.org/conference/usenixsecurity20/presentation/shen
M2Mon: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles	USENIX Sec	2021	https://www.usenix.org/system/files/sec21-khan-arslan.pdf
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors	USENIX Sec	2015	https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son.pdf
PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks	CCS	2015	https://dl.acm.org/doi/abs/10.1145/2810103.2813679?casa_token=Des4yGUU32IAAAAA:QlEruAEAaXbLIrNF685RR41L_2JzmpfRwNn6stY

			TJk0z3AQOYr2OhFrOxZMNVtbw--DLsHag35dg
Crystal (ball): I Look at Physics and Predict Control Flow! Just-Ahead-Of-Time Controller Recovery	ACSAC	2020	https://dl.acm.org/doi/pdf/10.1145/3274694.3274724
Securing Real-Time Microcontroller Systems through Customized Memory View Switching	NDSS	2018	https://chungkim.io/doc/ndss18-minion.pdf
Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach	CCS	2018	https://dl.acm.org/doi/pdf/10.1145/3243734.3243752
Cyber-Physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles	CCS	2020	https://dl.acm.org/doi/pdf/10.1145/3372297.3417249
SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants	USENIX Sec	2020	https://www.usenix.org/system/files/sec20-quinonez.pdf
Reverse Engineering and Retrofitting Robotic Aerial Vehicle Control Firmware using DisPatch	MobiSys	2022	https://dl.acm.org/doi/pdf/10.1145/3498361.3538938?casa_token=Uj1Arxz7h1AAAAA:TKOXPVJ1YqEeB_lKoCOeK5upoEWGxYZ4wCFPMcosZFNLPGfe2xQYSQJvamcuwg7bmsffzlqjjp9x
PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles	IEEE S&P	2022	https://www.cs.purdue.edu/homes/dxu/pubs/SP22_PGPATCH.pdf
PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles	NDSS	2021	https://kimhyungsub.github.io/NDSS21_hskim.pdf
From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY	USENIX Sec	2020	https://www.usenix.org/system/files/sec20-kim.pdf
Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks	ICRA	2018	https://www.cs.purdue.edu/homes/dxu/pubs/ICRA18_BlueBox.pdf