

Course Syllabus

[Jump to Today](#)



CDA5220.0V63: Foundations of Secure Execution Environment

Department of Computer Science,
College of Engineering and Computer Science

3 Credit Hours

Instructor Information

- Instructor: Yan Solihin
- Office Location: on Zoom or MS Teams
- Office Hours: right after class or by appointment
- Phone: 407-823-4191
- Digital Contact: yan.solihin@ucf.edu (<mailto:yan.solihin@ucf.edu>) or [Webcourses@UCF](#) messaging

Teaching Assistants

- GTA(s): None

Course Information

- Term: Spring 2023
- Course Number & Section: CDA 5220.0V63
- Course Name: Foundations of Secure Execution Environment
- Credit Hours: 3
- Class Meeting Days: TTh
- Class Meeting Time: 10:00 - 11:15am
- Class Location: online (Zoom)
- Course Modality: V

Enrollment Requirements

Course Prerequisites (if applicable): CDA 5106 or equivalent

Course Co-requisites (if applicable): N/A

Course Description

This class is a graduate course covering the foundations of secure execution environment (SEE). The course (1) equips students with foundational knowledge of threat models, root of trust, and types of attacks that can occur with the execution of programs in the cloud or at the edge nodes, and (2) equips students with principles of designing a secure execution environment, knowing what mitigation techniques are effective for specific attacks, and knowing how to reason about security-performance trade-offs.

Course Materials and Resources

Required Materials/Resources

- No required materials

Optional Materials/Resources

- John Paul Shen and Mikko Lipasti, “Modern Processor Design”, Waveland Press Inc., 2013
- Yan Solihin, “Fundamentals of Parallel Multicore Architecture”, CRC Press, 2016

Student Learning Outcomes

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

- Recall computer security concepts: Triad of security, trust/threat/security models, asset/participants/adversary, vulnerability/threats/attacks
- Analyze an appropriate trust model given a threat model
- Explain the pros and cons of various encryption modes
- [TBD] Recall differences in styles of ISAs and their pros and cons
- Recall various addressing modes
- Explain condition code, how instructions affect it, and how it is used for conditional branches
- Apply dependence analysis to identify WAW, WAR, RAW register dependences
- Given a list of conditional branch outcomes, show the final state of branch prediction table, for various branch predictors

- Given a list of instructions and their processing stage, show the state of reservation stations, load buffers, and ROB
- [TBD] Apply register renaming to eliminate false dependences
- Explain pros and cons of various cache inclusion policies
- Given a stream of memory accesses, show the final state of multi-level caches for various inclusion property policies
- Show how an address is translated from virtual to physical address, given a page table
- Explain the pros and cons of virtual vs. physical indexing, and virtual vs. physical tagging
- Given a list of memory accesses from different processor or cores, show step by step changes in cache states, for MESI coherence protocol
- Recall various types of memory fences and how they are used in processor
- Explain the pros and cons of direct vs. counter mode memory encryption
- Explain monolithic vs. split counter mode
- Explain counter replay attack
- Explain the differences between Merkle Tree, Bonsai Merkle Tree, and Counter Tree
- Explain persistent memory recoverability concept

Course Activities

The course will include:

- 1 to 2 programming assignments
- 5 to 10 quizzes
- Classroom presentation (presenting papers)
- Semester project, including final project presentation
- No extra credit will be given
- Students should have regular access to the internet and plan on logging into the course at least twice each week
- Students should plan on at least five hours' worth of homework outside of class each week).

Activity Submissions

Assignments should be submitted online through Webcourses@UCF

Attendance/Participation

Attendance is encouraged, but only required during the class meetings in which you are scheduled to present. If you will not be able to be present in class for your presentation, you must request rescheduling as soon as possible and no later than two weeks prior to your absence, unless an unforeseen conflict.

Make-up Exams and Assignments

Per university policy, you are allowed to submit make-up work (or an equivalent, alternate assignment) for authorized university-sponsored activities, religious observances, or legal obligations (such as jury duty). If this participation conflicts with your course assignments, I will offer a reasonable opportunity for you to complete missed assignments and/or exams. The make-up assignment and grading scale will be equivalent to the missed assignment and its grading scale. In the case of an authorized university activity, it is your responsibility to show me a signed copy of the Program Verification Form for which you will be absent, prior to the class in which the absence occurs. In any of these cases, please contact me ahead of time to notify me of upcoming needs.

Assessment and Grading Procedures

Assignment	Percentage of Grade
1 to 2 Programming Assignments	15% total
Quizzes	20% total
Paper presentation	15%
Project	50%
Total	100%

Letter Grade	Points
A	93 – 100 points

A-	90 – 92 points
B+	87 – 89 points
B	83 – 86 points
B-	80 – 82 points
C+	77 – 79 points
C	73 – 76 points
C-	70 – 72 points
D+	67 – 69 points
D	63 – 66 points
D-	60 – 62 points
F	59 and below

Consult the latest Undergraduate or Graduate [catalog \(http://catalog.ucf.edu/\)](http://catalog.ucf.edu/) for regulations and procedures regarding grading such as Incomplete grades, grade changes, and grade forgiveness.

Course Schedule

Please refer to the Course Schedule Page.

University Services and Resources

Academic Services and Resources

A list of available academic support and learning services is available at [UCF Student Services \(https://www.ucf.edu/services/\)](https://www.ucf.edu/services/). Click on "Academic Support and Learning Services" on the right-hand

<https://www.ucf.edu/services/>. Click on "Academic Support and Learning Services" on the right-hand side to filter.

Non-Academic Services and Resources

A list of non-academic support and services is also available at [UCF Student Services \(https://www.ucf.edu/services/\)](https://www.ucf.edu/services/). Click on "Support" on the right-hand side to filter.

If you are a UCF Online student, please consult the [UCF Online Student Guidelines \(https://www.ucf.edu/online/resources/guidelines/\)](https://www.ucf.edu/online/resources/guidelines/) for more information about your access to non-academic services.

Policy Statements

Academic Integrity

Students should familiarize themselves with [UCF's Rules of Conduct \(http://osc.sdes.ucf.edu/process/roc\)](http://osc.sdes.ucf.edu/process/roc). According to Section 1, "Academic Misconduct," students are prohibited from engaging in:

- *Unauthorized assistance*: Using or attempting to use unauthorized materials, information or study aids in any academic exercise unless specifically authorized by the instructor of record. The unauthorized possession of examination or course-related material also constitutes cheating.
- *Communication to another through written, visual, electronic, or oral means*: The presentation of material which has not been studied or learned, but rather was obtained through someone else's efforts and used as part of an examination, course assignment, or project.
- *Commercial Use of Academic Material*: Selling of course material to another person, student, and/or uploading course material to a third-party vendor without authorization or without the express written permission of the university and the instructor. Course materials include but are not limited to class notes, Instructor's PowerPoints, course syllabi, tests, quizzes, labs, instruction sheets, homework, study guides, handouts, etc.
- *Falsifying or misrepresenting* the student's own academic work.
- *Plagiarism*: Using or appropriating another's work without any indication of the source, thereby attempting to convey the impression that such work is the student's own.
- *Multiple Submissions*: Submitting the same academic work for credit more than once without the express written permission of the instructor.
- *Helping another violate* academic behavior standards.

For more information about Academic Integrity, students may consult [The Center for Academic](#)

Integrity [↗ \(https://academicintegrity.org/\)](https://academicintegrity.org/).

For more information about plagiarism and misuse of sources, see “**Defining and Avoiding Plagiarism: The WPA Statement on Best Practices** [↗ \(http://wpacouncil.org/node/9\)](http://wpacouncil.org/node/9)”.

Responses to Academic Dishonesty, Plagiarism, or Cheating

Students should also familiarize themselves with the procedures for academic misconduct in UCF’s student handbook, **The Golden Rule**. [\(http://goldenrule.sdes.ucf.edu/docs/goldenrule.pdf\)](http://goldenrule.sdes.ucf.edu/docs/goldenrule.pdf) UCF faculty members have a responsibility for students’ education and the value of a UCF degree, and so seek to prevent unethical behavior and when necessary respond to academic misconduct. Penalties can include a failing grade in an assignment or in the course, suspension or expulsion from the university, and/or a "Z Designation" on a student’s official transcript indicating academic dishonesty, where the final grade for this course will be preceded by the letter Z. For more information about the Z Designation, see **The Golden Rules** [\(http://goldenrule.sdes.ucf.edu/zgrade\)](http://goldenrule.sdes.ucf.edu/zgrade).


Course Accessibility Statement

The University of Central Florida is committed to providing access and inclusion for all persons with disabilities. Students with disabilities who need disability-related access in this course should contact the professor as soon as possible. Students should also connect with **Student Accessibility Services** [\(http://sas.sdes.ucf.edu/\)](http://sas.sdes.ucf.edu/) (Ferrell Commons 185, [sas@ucf.edu \(mailto:sas@ucf.edu\)](mailto:sas@ucf.edu), phone (407) 823-2371). Through Student Accessibility Services, a Course Accessibility Letter may be created and sent to professors, which informs faculty of potential access and accommodations that might be reasonable. Determining reasonable access and accommodations requires consideration of the course design, course learning objectives and the individual academic and course barriers experienced by the student.

Campus Safety Statement

Emergencies on campus are rare, but if one should arise in our class, everyone needs to work together. Students should be aware of the surroundings and familiar with some basic safety and security concepts.

- In case of an emergency, dial 911 for assistance.
- Every UCF classroom contains an emergency procedure guide posted on a wall near the door. Please make a note of the guide’s physical location and consider reviewing the online version at **UCF Emergency Information** [\(http://emergency.ucf.edu/emergency_guide.html\)](http://emergency.ucf.edu/emergency_guide.html).

- Students should know the evacuation routes from each of their classrooms and have a plan for finding safety in case of an emergency.
- If there is a medical emergency during class, we may need to access a first aid kit or AED (Automated External Defibrillator). To learn where those items are located in this building, see <http://www.ehs.ucf.edu/workplacesafety.html> (<http://www.ehs.ucf.edu/Workplacesafety>) (click on link from menu on left).
- To stay informed about emergency situations, sign up to receive UCF text alerts by going to my.ucf.edu (<http://my.ucf.edu>) and logging in. Click on "Student Self Service" located on the left side of the screen in the tool bar, scroll down to the blue "Personal Information" heading on your Student Center screen, click on "UCF Alert," fill out the information, including your e-mail address, cell phone number, and cell phone provider, click "Apply" to save the changes, and then click "OK."
- Students with special needs related to emergency situations should speak with their instructors outside of class.
- To learn about how to manage an active-shooter situation on campus or elsewhere, consider viewing this video.
[You CAN Survive an Active Shooter](https://youtu.be/NIKYajEx4pk)  (<https://youtu.be/NIKYajEx4pk>)



(<https://youtu.be/NIKYajEx4pk>)

Deployed Active Duty Military Students

If you are a deployed active duty military student and feel that you may need a special accommodation due to that unique status, please contact your instructor to discuss your circumstances.

Copyright

This course may contain copyright protected materials such as audio or video clips, images, text materials, etc. These items are being used with regard to the Fair Use doctrine in order to enhance the learning environment. Please do not copy, duplicate, download or distribute these items. The use of these materials is strictly reserved for this online classroom environment and your use only. All copyright materials are credited to the copyright holder.






Third-Party Software and FERPA










During this course you might have the opportunity to use public online services and/or software applications sometimes called third-party software such as a blog or wiki. While some of these could be required assignments, you need not make any personally identifying information on a public site. Do not post or provide any private information about yourself or your classmates. Where appropriate you may use a pseudonym or nickname. Some written assignments posted publicly may require personal reflection/comments, but the assignments will not require you to disclose any personally identity-sensitive information. If you have any concerns about this, please contact your instructor.

Third-Party Accessibility and Privacy Statements

TBD

Course Summary:

Date	Details	Due
Wed Oct 23, 2019	 Programming Assignment 1 - Creating an Intel SGX Enclave (https://webcourses.ucf.edu/courses/1425296/assignments/7855339)	due by 11:59pm
Fri Oct 25, 2019	 Reading List Presentation Sign Up (https://webcourses.ucf.edu/courses/1425296/assignments/7855344)	due by 11:59pm
Wed Oct 30, 2019	 Quiz 7 - Memory Encryption and Integrity Verification (https://webcourses.ucf.edu/courses/1425296/assignments/7855335)	due by 11:59pm
Mon Nov 4, 2019	 Programming Assignment 2: Working with two Enclaves (https://webcourses.ucf.edu/courses/1425296/assignments/7855340)	due by 11:59pm
Wed Nov 13, 2019	 Programming Assignment 3: Establishing Trust (Measurement, Attestation, and Sealing) (https://webcourses.ucf.edu/courses/1425296/assignments/7855341)	due by 11:59pm

Fri Nov 22, 2019	 Presentation upload option for students who do not get to present in class (https://webcourses.ucf.edu/courses/1425296/assignments/7855338)	due by 11:59pm
<hr/>		
Wed Dec 4, 2019	 Semester Project (https://webcourses.ucf.edu/courses/1425296/assignments/7855345)	due by 11:59pm
<hr/>		
Wed Nov 23, 2022	 Quiz 6 - OOO (https://webcourses.ucf.edu/courses/1425296/assignments/7939050)	due by 11:59pm
<hr/>		
Thu Jan 26, 2023	 Principle of Adequate Protection (https://webcourses.ucf.edu/courses/1425296/assignments/7855337)	due by 11:59pm
<hr/>		
Tue Feb 7, 2023	 Rethinking Threat and Trust Model (https://webcourses.ucf.edu/courses/1425296/assignments/7932992)	due by 11:59pm
<hr/>		
Tue Feb 7, 2023	 Quiz 1 - Instruction Set Architecture (https://webcourses.ucf.edu/courses/1425296/assignments/7936814)	due by 11:59pm
<hr/>		
Thu Feb 9, 2023	 Quiz 2 - Pipelining and Branch Prediction (https://webcourses.ucf.edu/courses/1425296/assignments/7939049)	due by 11:59pm
<hr/>		
Tue Feb 14, 2023	 Quiz 3 - Cache (https://webcourses.ucf.edu/courses/1425296/assignments/7936815)	due by 11:59pm
<hr/>		
Thu Feb 16, 2023	 Quiz 4 - Cache Coherence and Memory Consistency (https://webcourses.ucf.edu/courses/1425296/assignments/7855334)	due by 11:59pm
