Software Security

CIS 4930

Class Periods:

Tuesday | Period 7 | 1:55pm - 2:45pm

Thursday | Periods 7-8 | 1:55pm - 3:50pm

Location: CSE E121

Academic Term: Spring 2020

> "It is the one who does the work that does the learning"
>
> *–Terry Doyle*

Instructor:

Byron J. Williams, Ph.D.

byron@cise.ufl.edu

352-294-1017

Office Hours: Tue 3:00-4:00pm; Thursday 1:00-1:45pm; Other times by appointment - Materials Engineering Building (MAE) 205B

Teaching Assistant/Peer Mentor/Supervised Teaching Student:

Can also be reached on Slack

- Anurag Yadav anuragswar.yadav@ufl.edu - Office Hours - TBD
- Blas Kojusner - bkojusner@ufl.edu - Office Hours - Wednesdays 12:50 - 2:45 in CSE E309

Course Description

The Software Security course focuses on teaching students the fundamentals of application security with the aim of providing a foundational level of knowledge matched with offensive and defensive skills developed through hands-on experience. Students will learn the basics of software security, common vulnerabilities and attacks, threat modeling, the secure development lifecycle, and more while receiving hands-on practice in both exploitation techniques and strategies for protecting and hardening applications. The theoretical portions of the course will focus strongly on secure design as a means of enabling developers to create robust, secure applications. Developed through a partnership between Facebook and CodePath, the course introduces a wide range of topics via a combination of sessions and labs, giving students both a thorough foundation in the details of software security and an introduction to the broader landscape of information security. The Codepath material consists of 12-week of lab and capture the flag exercises. Students are required to register with Codepath for this portion of course material. This course is not a comprehensive intro to cybersecurity. Rather, our focus is on the design and security of software systems (particularly web and distributed systems).

Course Pre-Requisites / Co-Requisites

Senior Standing unless approved by instructor

Students should...

have introductory knowledge of:

- engineering and programming
- web applications and web development
- middleware such as web servers and databases

be pursuing (or have previously completed) a course of study related to **computer science** that includes:

- fundamental CS concepts such as data structures and algorithms
- hands-on programming/scripting experience
- application development and design.

Course Outcomes & Objectives

The course allow students to develop the mindset of a security professional along with understanding the fundamentals of software security that is enabled by secure design. Students will study common application vulnerabilities and be provided hands-on practice writing exploits and domain-driven defensive strategies. Tuesday classes will focus on software security theoretical concepts. Thursday classes are designed for lab work.

Required Textbooks and Software

Notes derived from literature sources will be presented in class (lecture slides). Required readings from various sources (academic literature, magazines, blog posts, Codepath) will be announced in class and posted on Canvas and/or in the course Slack channel (drbyron.slack.com).

Students must register with codepath.org/classes (Cybersecurity and Hacking) to gain access to the 12-week lab / CTF assignments and materials provided in their learning portal. Student must have a Github account to register.

Apply Here: https://apply.codepath.org/cohorts/university-cybersecurity-spring-2020/versions/student/

OPTIONAL: J. Ransome and A. Mistra, "Core Software Security," Auerbach Publications; 1st edition, Dec 2013, ISBN-13: 978-1466560956.

Communication & Email Policy

All email communication with the instructor should be sent to byron@cise.ufl.edu from student .ufl email accounts. We will use Slack to communicate regarding the Codepath labs and other course assignments. Students will be sent Slack invitations the first week of class.

Professional Component (ABET):

The following lists the contribution of the course to meeting the professional components of the ABET-accredited degree.

Relation to Program Outcomes (ABET):

Outcome	Coverage*
1. An ability to identify, formulate, and solve engineering problems by applying principles of engineering, science, and mathematics.	Medium
2. An ability to apply both analysis and synthesis in the engineering design process, resulting in designs that meet desired needs.	Medium
3. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions.	High
4. An ability to communicate effectively with a range of audiences	Low
5. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.	Medium
6. An ability to recognize the ongoing need for additional knowledge and locate, evaluate, integrate, and apply this knowledge appropriately.	High
7. An ability to function effectively on teams that establish goals, plan tasks, meet deadlines, and analyze risk and uncertainty	Low

*Coverage is given as high, medium, or low. An empty box indicates that this outcome is not covered or assessed in the course.

Course Schedule

The following unordered lists of topics will be covered in the course. Assigned reading, related lectures slides / notes, and dates will be posted to Canvas / Slack.

Secure Design
- Security as a Concern not a Feature
- Domain-Driven Design
- Secure Code Constructs
- Software State (complexity & integrity)
- Software Delivery Pipeline (DevSecOps)
- Handling Failures
- Cloud Thinking
- Legacy Code
- Best Practices

Software Security
- Fundamental Security Principles
- Secure development lifecycle
- Security architectures
- Threat modeling

Attacks / Exploits:
- Data Exposures
- Social Engineering
- Cross-Site Scripting
- Basic Cryptography & Encryption
- Malicious Input/Output Attacks
- User Authentication
- Network Security
- Footprinting and Forgery
- Honeypots
- Session Hijacking and Fixation
- The Secure Web
- Common Attacks and Prevention (OWASP Top 10+)
- White Hat / Black Hat hackers
- Security tools

* plus additional sub-topics related to what's listed above

Attendance Policy, Class Expectations, and Make-Up Policy

Class attendance is mandatory. Attendance will be tracked using roll call / signature form. Unexcused absences

Excused absences must be consistent with university policies in the undergraduate catalog (https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx) and require appropriate documentation. It is your responsibility to contact the professor to make up work missed due to an excused absence when you return to class.

CodePath Policy

CodePath courses focus on developing student's habits and skills in order to to be successful in the tech industry. Success in industry goes beyond proficiency in technical domains; The ability to be punctual, meet project deadlines and work effectively in a collaborative team are equally important skills. The following policies around attendance and coursework submissions are meant to encourage professional behavior.
See: https://courses.codepath.org/snippets/cybersecurity_university/syllabus_spring_2020

Attendance is a reflection on your professionalism. Each class is a professional appointment that you have with the instructor and your classmates. If you cannot make an appointment, then the professional thing to do is to cancel the appointment in advance. Please notify Dr. Williams of the circumstances for each absence/ tardiness by email prior to class. No excused absences will be given without advanced noticed (certain exceptions apply).

Evaluation of Grades

Assignment	Percentage of Final Grade
CodePath Coursework (see: https://courses.codepath.org/snippets/cybersecurity_university/grading)	70%
Quizzes and Mini-Projects	15%
Experience Reports	15%
	100%

CodePath Coursework - 13 Weekly Codepath Labs, Assignments, and CTFs (70%+):
The Codepath repo will contain 13 weekly labs and assignments that will apply methods / techniques covered in the course material. All assignments / labs must be completed. Late assignments will be penalized. Each assignment / lab (with exceptions for capstone assignments) are due on Wednesday night at 11:59pm. Assignments will be submitted online via Github (each student is required to have a github.com account) and a Security Shepard account. Each lab contains required and optional challenges. Optional challenges and extension projects can be done for full to extra credit for each assignment. Students are allowed to earn extra credit for the Codepath material up to 74% of the final grade (able to obtain 1 extra credit point for each type of Codepath assessment [labs, CTF, capstone, assignments]).

See CodePath Course Overview (only available after registration) - https://courses.codepath.org/snippets/cybersecurity_university/syllabus_spring_2020

Student Experience Reports: Students will write 1-2 page experience reports (up to 3) to answer questions posed on the lecture and lab material.

Quizzes & Mini-Projects: Short pop quizzes and mini-projects to implement solutions for the exploits covered (e.g., implement login page to hash/salt stored passwords, form input validation, etc).

Exams: There will be no exams

Grading Policy
The following grade scale will be used to assign final grades. There will be no rounding up (i.e., a final score of 93.3 is an A-)

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at: https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Instructor Office Location for Office Hours and Scheduled Appointments

Students Requiring Accommodations

Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at https://evaluations.ufl.edu/evals. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at https://evaluations.ufl.edu/results/.

University Honesty Policy
UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment
The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:
• Your academic advisor or Graduate Program Coordinator
• Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
• Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
• Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use
All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy
There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.