UF Herbert Wertheim College of Engineering
Department of Computer & Information Science & Engineering
UNIVERSITY of FLORIDA

CODEPATH*ORG

facebook

Software Security
CIS 4930/6930

Syllabus Spring 2019

Instructor: Dr. Byron J. Williams
Email: byron@cise.ufl.edu
Office: MAE 205B
Office Hours: Tue 3:00-4:00pm; Wednesday 2:00-3:00pm; Other times by appointment
Course Periods: Tue: Period 7 - 1:55pm - 2:45pm
Thur: Period 7-8 - 1:55pm - 3:50pm (Codepath Course Material)
Location: CSE E119
Final Exam: 5/01/2019 @ 10:00 AM - 12:00 PM

Teaching Assistants (Please contact using Canvas):

- Sanaz Gheibi - sgheibi@ufl.edu - Office Hours - TBD
- Anurag Yadav - anuragswar.yadav@ufl.edu - Office Hours - TBD

Course Overview

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. 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.

Course Outcomes: The course allow students to develop the mindset of a security professional along with understanding the fundamentals of software security, common application vulnerabilities, and provides hands-on practice focused. Tuesday classes will focus on software security theoretical concepts. Thursday classes are designed for student presentation and lab work.

Course Topics (not ordered):

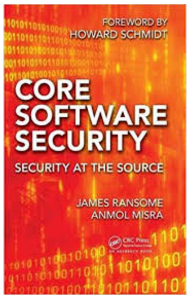
- Fundamental Security Principles
- Secure development lifecycle
- Social Engineering
- Security architectures
- Threat modeling

- Input/Output Attacks
- Footprinting and Forgery
- Session Hijacking and Fixation
- Encryption and User Authentication
- User Authentication Attacks
- The Secure Web
- Securing Servers & Development Operations
- Assessment and Monitoring
- Common Attacks and Prevention (OWASP Top 10+)

Prerequisite / Expectations: Senior standing (recommended)

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.



Texts and other requirements

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

Students must register with codepath.org (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. Other required readings from various sources (academic literature, magazines, blog posts) will be announced in class. (**APPLY HERE** http://bit.ly/2RfzWUZ)

Assessment & Grades

12 Weekly Codepath Labs, Assignments, and CTFs (60%+)

The CodePath repo will contain 12 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 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 65% of the final grade (extra credit scale based on range of student scores).

See CodePath Repo - See https://courses.codepath.com/courses/cybersecurity_university/

Student Presentations & Demos (10% - Group - CIS 4930)

Students will give one group presentation discussing and demonstrating a course topics. Demonstrations will closely follow Codepath material and weekly lab setup and include some additional topics.

Research Paper & Presentation (10% - Group - CIS 6930)

Graduate students will write a review paper on an agreed upon topic and present the results to class.

Exams (Mid-term & Final) (26%)

There will be two closed-book exams covering lecture topics, in-class discussion, and lab material.

Quizzes (4%)

Quizzes given randomly during regular class time to evaluate student assigned reading and

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is required for all class periods. Tuesday lectures may include pop quizzes covering prior lecture material. Missed quizzes cannot be made up without an excused absence. Cell phones are not to be used in class.

Thursday lab session attendance will impact the CodePath course grade. The CodePath Attendance policy below:

CodePath Attendance (Thursday Sessions)

- 10% of the final grade is based on attendance.
- Perfect attendance (attendance at all sessions) will result in a 5% bonus to the final grade.
- 2 absences are allowed without penalty, no questions asked.
- Each additional absence beyond the allowed 2 absences will incur a 2% deduction off the final grade up to a maximum of 10%.

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.

Communications Policy

We will use Canvas to facilitate **all course communications** particularly any communication discussing assignments, grades, or any coursework. UF email addresses / accounts should be used for all other course and faculty/student communication. Canvas chat will be open for students having trouble completing the weekly labs. Students are encouraged to help one another by explaining concepts required to solve the lab assignments. Students should not share answers (see University Honesty Policy below).

Time Commitment

- In-person class session attendance: Classes meet 2x per week - Tuesday Session (1-hr) is lecture and in-class activity - Thursday session (~2hr) is student presentations and lab / CTF assignments during 12-week Codepath lab period (starts 2nd week of class).
- Student's should plan to spend 5-10+ hours outside of class working on coursework and readings.

CodePath: 12 Week Lab + CTF Sub-Course (starts 2nd week of class)

CodePath holds all professional and university students to the same high bar of quality course work and professionalism. In order to be considered CodePath alumni and receive recognition for successful completion of the course from CodePath, **students must complete the course with a final score of 70% or above**.

- Students meeting the above requirements will:
  1. Receive a CodePath certificate of completion with mentions of any awards achieved in the course.
  2. Be considered CodePath alumni and gain access to alumni networks.
  3. Gain full access to the CodePath career center and be eligible for mentorship opportunities with CodePath professional alumni.
- Students who complete the course with a final score of 85% and above are considered to be honors students and will have this reflected on their certificates

Codepath Lab / CTF Coursework Weighting - 60% of Final Grade

All Codepath coursework grading and accountability is handled by CodePath. The following table outlines how each coursework section is weighted in calculating a student's final grade. See Coursework Grading for a breakdown of scores for individual coursework items.

Weight	Section	Description
20%	Labs	Security Shepherd Platform
30%	CTFs	Weekly CTF Platform
30%	Assignments	Pen-testing
10%	Capstone CTF	Capstone CTF Platform
10%	Attendance	Professionalism

CodePath Coursework Grading - https://courses.codepath.com/snippets/cybersecurity_university/grading

Participation (in-class, Facebook group, Codepath discussion board, Course Canvas channel)

Students are required to read assigned material in advance and participate in Facebook community discussion (posting and answering questions), the discussion board (sharing answers / tips), and course Canvas chat channel.

SEE Full CodePath Syllabus and Course Overview Here:
https://courses.codepath.com/courses/cybersecurity_university/pages/bootcamp_structure?renderer=cm

UF Final Grading & Course Policy

The final grade will be determined by the following weights.

CIS 4930 - Undergraduate	CIS 6930 - Graduate
26% Exams (Individual)	26% Exams (Individual)
10% Group Presentation / Demo	10% Research Paper & Presentation
60% Codepath Labs, Assignments & Capstone **(SEE ABOVE *Coursework Weighting*)**	60% Codepath Labs, Assignments & Capstone **(SEE ABOVE *Coursework Weighting*)**
4% Lecture Quizzes & Participation	4% Lecture Quizzes & Participation

Grading Scale

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

HWCOE Recommended Content

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

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://www.dso.ufl.edu/sccr/process/student-conduct-honor-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.

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: http://registrar.ufl.edu/catalog0910/policies/regulationferpa.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 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.

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@ufl.edu

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

Appendix A

Codepath Course Content

Week 1 - Data Exposures
Reading:

- Security Introduction
- Castles and Heist Films
- Fundamental Security Principles
- Request methods and headers
- Attack: URL Manipulation
- Attack: Insecure Direct Object Reference

Lab:

- Hands on with URL Manipulation and IDOR

Week 2 - Malicious Input
Reading:

- Attack: SQL Injection (SQLI)
- Validating input
- Sanitizing incoming data
- Attack: File Upload Abuse
- Attack: Remote Code Execution

Lab:

- Hands on with SQLI and RCE exploits

Assignment:

- Capture The Flag (CTF): SQLI and RCE exploits

Week 3 - Cross-Site Scripting
Reading:

- Attack: Cross-Site Scripting (XSS)
- Sanitizing outgoing data
- Attack: Clickjacking

Lab:

- Hands on with XSS and clickjacking exploits

Assignment:

- Capture The Flag (CTF): XSS and clickjacking exploits

Week 4 - Cookie and Session Based Attacks

Reading:

- Attack: Faked Requests
- Cookies and Sessions
- Attack: Cookie Theft and Manipulation
- Attack: Cross-Site Request Forgery (CSRF)
- Attack: Session Hijacking
- Attack: Session Fixation

Lab:

- Hands on with CSRF exploits
- Learn design pattern for implementing CSRF tokens
- Hands on with Session Hijacking and Session Fixation exploits

Assignment:

- Capture The Flag (CTF): CSRF exploits

Week 5 - Cryptography

Reading:

- Encryption
- Attack: Brute Force Attack
- Attack: Dictionary Attack

Lab:

- Identify and exploit weak cryptographic protection
- Identify and exploit poorly-implemented crypto
- Using PGP / GPG

Assignment:

- Capture The Flag (CTF): Identify and exploit weak cryptographic protection and poorly-implemented crypto

Week 6 - User Authentication

Reading:

- User Authentication
- Strong Passwords
- Password Managers
- Multi-Factor Authentication
- Attack: Username Enumeration
- Attack: Credential Theft
- Phishing
- Data breaches
- Attack: Privilege Escalation

Lab:

- Login page vulnerabilities and exploits
- Password reset vulnerabilities and exploits
- Hash cracking with hashcat

Week 7 - White Hat, Black Hat

Reading:

- Attack: Footprinting, Enumeration, and Fingerprinting
- Code Reading and Analysis

Lab:

- Understanding VMs and containers
- Setting up WordPress in a VM/container
- Setting up Kali in a VM/container
- Using wpscan to discover and recreate known WP issues

Assignment:

- Research vulnerabilities in older WP versions
- Recreate exploits using Kali and other tools
- Documenting research and submitting proof of work

Week 8 - Better Tools, Better Targets

Lab:

- Using Metasploit to attack WP
- Using Meterpreter and reverse shells
- Using sqlmap

Week 9 - NetSec

Reading:

- Netsec Crash Course
- Firewalls
- Intrusion Detection Systems
- Risk Assessment
- Penetration Testing
- Threat Monitoring
- Incident Response

Lab:

- Basic networking tools
- Basic packet analysis
- Installing and using Wireshark
- Malware traffic analysis
- WiFi Cracking

Assignment:

- Build a Honeypot
- Intrusion Detection

Week 10 - Social Engineering

Reading:

- Social Engineering Strategies
- Case Studies
- Attack: Social Engineering - Pretexting
- Attack: Social Engineering - Baiting
- Attack: Social Engineering - Phishing
- Attack: Social Engineering - Quid Pro Quo
- Attack: Social Engineering - Tailgating
- Insider Threats, Contractors

Lab:

- Using Social Engineering Toolkit

- Phishing via email
- Fake Login page
- Simulated Phishing Exercise

Weeks 11 & 12 - Capture The Flag

- Mutli-week, multi-team CTF competition
- Live web targets at various difficulties
- Student-supplied targets
- Quiz questions