CityUniversity of Seattle | CityU.edu

Syllabus

CY488: SOFTWARE SECURITY

School of Technology & Computing

3 Credits
Summer2022

Access to the Internet is required.
All written assignments must be in Microsoft-Word-compatible formats.
See the library's APA Style Guide tutorial for a list of resources that can help you use APA style.

Faculty Information

Professional experience information for instructors is found under *Faculty Information* in the online course menu.

Contact Information

Contact information for instructors is found under *Faculty Information* in the online course menu.

Email: [first name]
Phone: [xxx-xxx-xxxx]
Office Hours and Response Time: [I am available through MS Teams XXday and XXday nights between x-p.m.- x-p.m. I will respond within 24 hours. I will grade within 3 business days after the due date.]
Bio: (keep images under 300px wide)

Course Description

This course covers the principles and practices of secure programming. The course covers coding practices that avoid introducing vulnerabilities that could be exploited. The course also covers the incorporation of security features and services such as encryption, authentication, and access control, which allow the creation of a secure system. Virtual labs are included to provide students with "hands-on" experience in configuring, hardening, and deploying virtual devices, such as web servers, to understand and combat common exploits. Students must be familiar with basic programming concepts such as syntax, structure, control-of-flow, program problem solving, as well as computing resources.

Course Resources

Required and recommended resources to complete coursework and assignments are found on the course Reading List. The reading list can be found under Course Information in Blackboard as well as from the library homepage.

Note: Required resources that must be purchased by the student are tagged “Purchase from a vendor of your choosing.” Required resources with a direct link, “Available through CityU Library”, are available at no cost to students.

Students in Canada will see required resources they need to purchase tagged “Purchase from the Canadian Bookstore.” Students outside the U.S. and Canada should contact their advisor or textbook coordinator for additional information.

Course Outcomes

This course will prepare students to:

- Understand how to develop robust and secure software applications by identifying a standard set of policies, best practices, design patterns, and guidelines.
- Apply the threat characteristics to balance between usability and security of applications.
- Analyze policies for implementing updates, activations, patches, releases, and other real-time application deployment issues that compromise system security and stability.
- Evaluate appropriate countermeasures after identifying the common vulnerabilities, threats, and attack vectors in the programming context.
- Create secure systems and programs by using the secure software life cycle from the beginning to the end to write, test, and debug programs.

Additional Information

- **Introduction**
  - The Importance and Relevance of Software Security
  - Software Security and the Software Development Lifecycle
  - Quality Versus Secure Code
  - The Three Most Important SDL Security Goals
  - Threat Modeling and Attack Surface Validation
  - Chapter Summary—What to Expect from This Book
- **The Secure Development Lifecycle**
  - Overcoming Challenges in Making Software Secure
  - Software Security Maturity Models
  - ISO/IEC 27034—Information Technology—Security Techniques—Application Security
  - Other Resources for SDL Best Practices
  - Critical Tools and Talent
  - Principles of Least Privilege
  - Privacy
  - The Importance of Metrics
  - Mapping the Security Development Lifecycle to the Software Development Lifecycle
  - Software Development Methodologies
- **Security Assessment (A1): SDL Activities and Best Practices**
  - Software Security Team Is Looped in Early
  - Software Security Hosts a Discovery Meeting
  - Software Security Team Creates an SDL Project Plan
  - Privacy Impact Assessment (PIA) Plan Initiated
  - Security Assessment (A1) Key Success Factors and Metrics
- **Architecture (A2): SDL Activities and Best Practices**
  - A2 Policy Compliance Analysis
  - SDL Policy Assessment and Scoping
  - Threat Modeling/Architecture Security Analysis

- Open-Source Selection
- Privacy Information Gathering and Analysis
- Key Success Factors and Metrics

- **Design and Development (A3): SDL Activities and Best Practices**
  - A3 Policy Compliance Analysis
  - Security Test Plan Composition
  - Threat Model Updating
  - Design of Security Analysis and Review
  - Privacy Implementation Assessment
  - Key Success Factors and Metrics
- **Design and Development (A4): SDL Activities and Best Practices**
  - A4 Policy Compliance Analysis
  - Security Test Case Execution
  - Code Review in the SDLC/SDL Process
  - Security Analysis Tools
- **Ship (A5): SDL Activities and Best Practices**
  - A5 Policy Compliance Analysis
  - Vulnerability Scan
  - Penetration Testing
  - Open-Source Licensing Review
  - Final Security Review
  - Final Privacy Review
- **Post-Release Support (PRSA1–5)**
  - Right-Sizing Your Software Security Group
  - PRSA1: External Vulnerability Disclosure Response
  - PRSA2: Third-Party Reviews
  - PRSA3: Post-Release Certifications
  - PRSA4: Internal Review for New Product Combinations or Cloud Deployments
  - PRSA5: Security Architectural Reviews and Tool-Based Assessments of Current, Legacy, and M&A Products and Solutions
- **Applying the SDL Framework to the Real World**
  - Build Software Securely
  - Determining the Right Activities for Each Project
  - Architecture and Design
  - Testing
  - Agile: Sprints
- **Pulling It All Together: Using the SDL to Prevent Real-World Threats**
  - Strategic, Tactical, and User-Specific Software Attacks
  - Overcoming Organizational and Business Challenges with a Properly Designed, Managed, and Focused SDL
  - Software Security Organizational Realities and Leverage
  - Overcoming SDL Audit and Regulatory Challenges with Proper Governance Management
  - Future Predictions for Software Security

Grading Scale

The grades earned for the course will be calculated using City University of Seattle's decimal grading system, found in the current University Catalog (https://www.cityu.edu/catalog/).

Grading rubrics with details on how each assignment will be graded are located under *Assignments* and/or in *My Grades* in the online course menu. Students should review each assignment's rubric before completing their work to understand how it will be assessed.

OVERVIEW OF REQUIRED ASSIGNMENTS	% OF FINAL GRADE	POINTS
Instructor Determined Assignments	***30%***	
The Muddiest Point (MP)	5%	50 = 5 points * 10 modules
Concept Test (CT)	5%	50 = 5 points * 10 modules
Discussion Board (DB)	10%	100 = 10 points * 10 modules
Knowledge Check (KC)	10%	100= 10 points * 10 modules
Major Assessments	***70%***	
Hands-On-Skill (HOS)	10%	100= 10 points * 100 modules
Virtual Lab (VL)	30%	300= 30 points * 10 modules
Team Project (RP)	30%	Proposal: 30 points Progress: 70 points Final Report: 120 points Final PPT: 80 points Subtotal: 300 points
TOTAL	**100%**	**1,000 points**

Course Assignments and Grading

The instructor will provide grading rubrics that will explain how this assignment will be graded.

The Muddiest Point (MP)

Before class, students are required to submit the Muddiest Point (MP) activity. The purpose of this activity is to stimulate student engagement. The instructor uses the MP to assess how students understood the required readings. The instructor also uses the MP to customize the lecture scope to implement Just-in-Time Teaching (JiTT). The MP consists of writing a brief reflective essay (<= 50 words) identifying the most confusing part (i.e., the MP) of the content covered in the upcoming module. If a student understood all concepts, the student needs to explain the most exciting aspect. There is one multiple-choice question from the required reading to demonstrate that the student understood the required readings.

Criteria	***% of Grade***
Participation	80%
Accuracy	20%
TOTAL	**100%**

Concept Test (CT)
The instructor poses a problem based on the key concepts of a lecture. After reflecting on the problem, students submit their responses, and the instructor reviews them without providing a correct answer. Students discuss their thought process and solution with a peer. Students then commit to an answer and re-submits their responses. Instructor reviews responses and thought processes with the correct answer.

Criteria	***% of Grade***
Engagement	100%
TOTAL	**100%**

Discussion Board (DB)
All classes are required to use the Discussion Board. Participation through DB is an integral part of this course. It is defined as active engagement in a discussion or other activity. Instructors will determine the type of activities and their due dates; moreover, different DB activities will have different substance and length guidelines. The instructor will provide specific instructions to students.

A student posts an answer to a weekly discussion topic in Discussion Board. The student also posts a response to two other students' posts by the end of each module. Comments and questions should be clear and thoughtful, with correct grammar, spelling, and punctuation. The instructor will grade the quality of your discussion postings on both content and response.

Questions or comments specifically for the instructor should be emailed directly to the instructor or posted in the Question and Answer Forum. Students who want to talk with other students about issues unrelated to the discussion forums should use the Coffee Talk Forum.

Although your DB postings' tone can be informal, your instructor will expect the content to be on a professional level. Your comments and questions for discussion should be clear and thoughtful, with correct grammar, spelling, and punctuation. As with written assignments, your discussion postings' quality will be graded on both content and presentation.

Criteria	***% of Grade***
Participation	50%
Writing	50%
TOTAL	**100%**

Hands-on Skill (HOS)
The instructor will assign hands-on skill exercises to a pair of students in class or individually online. Students pair up and practice exercises to learn specific programming languages, application programming interfaces (APIs), or tools related to the programming assignments or virtual labs. Two quizzes measure hands-on skills acquired.

Criteria	*% of Grade*
Practice Exercise	70%
Engagement	20%
Correctness	10%
TOTAL	**100%**

Virtual Lab (VL)

Students complete cloud-based labs that support the concepts taught within the course. VLs involve viewing instructional documents and following systematic instructions. Activities are embedded within each lab. The activities present a challenge to complete. Each lab is graded on accuracy and writing. A student has unlimited attempts at each lab to increase their accuracy and learn the required skills. Reports submitted include a write up on their understandings and findings in their lab reports.

Criteria	*% of Grade*
Accuracy	80%
Writing	20%
TOTAL	***100%***

Knowledge Check (KC)

Weekly quizzes measure knowledge concepts acquired. Focus on the underlying principles and concepts rather than memorization to solve the quizzes.

Criteria	*% of Grade*
Correctness	100%
TOTAL	**100%**

Team Project (TP)

Project Description: Case Study

In the security research paper, the student will analyze how cloud-based Serverless computing impacts its security development in general. The student reflects on security principles, researches the current adversarial environment, identifies system vulnerabilities subject to exploitation in the serverful environment, and explores remedies to thwart these threats in the serverless computing environment. For example, a student can research Serverless computing architecture security and quality analysis for back-end development or on software quality and security can be improved using the serverless computing technology.

Each student can select his or her team that consists of three to four students. A group of fewer than three students requires the instructor's approval. Each team will use an instructor-approved topic relevant to the course.

The paper must be no less than 6-7 pages. We required students to use the paper template from EDSIG/CONISAR, the international conference standard. *The instructor may recommend the best papers in this course to conferences with your team's approval. If necessary, the instructor may require more revisions after the course is over. However, the paper submission is optional and has nothing to do with your course grade*.

We will provide you three report templates and one presentation template. The file name consists of team project number, team number, and the list of your team members. For example, "*TP01 T03 Sam John Mark*."

- TP01 for the proposal - "*TP01 T0X Author1 Author2 Author3.docx*"
- TP02 for the progress report - "*TP02 T0X Author1 Author2 Author3.docx*"
- TP03 for the final report - "*TP03 T0X Author1 Author2 Author3.docx*"
- TP04 for the final presentation slide - "*TP04 T0X Author1 Author2 Author3.pptx*"

As in any scholarly writing, students should not merely copy information from another author. Students should use evidence to support the contentions they have drawn from their findings and critically analyze related literature. In essence, each paper needs to be an analytical paper, not a summary of readings.

In addition, a team presentation slide is required.

- The presentation consists of 15+4 slides: 15 slides for content and 4 slides for cover, agenda, key reference, and Q&A.
- The PPT template is provided. Your team can change design and color for your team's purpose.
- If necessary, a presentation video (15 minutes) may be requested.
- If necessary, a demo video (a maximum of 1-2 minutes) may be requested. But, the demo time should be included the total presentation time (15 minutes).

Four submissions are required according to the following schedule:

- Proposal (1 page; 30 points) - Starting (Module 1) & Ending (Module 3)
- Progress Report (3-4 pages; 70 points; graded after the proposal has been submitted) - Starting (Module 4) & Ending (Module 7)
- Final Report (6-7 pages; 70 points; graded after the progress has been submitted) - Starting (Module 8) & Ending (Module 10)
- Final PPT (15+4slides, 30 points; graded after the final report has been submitted) - Starting (Module 8) & Ending (Module 10)

Students are expected to use the assigned readings, videos, and other materials throughout the quarter. Students will need to utilize additional sources that were not assigned by the professor. While stylized after an industry report, nonetheless, students are expected to employ APA formatting of citations, footnotes, and bibliography. Students must cite the sources of all ideas, facts, and information used that are not their own, even if they have put the information into their

own words. Failure to do so is plagiarism, although the oversight is unintentional. To avoid plagiarism, check "Avoid Plagiarism."

Proposal

- Identify which of the case studies provided by you and you will be using for your Security Research Paper.
- Write a methodology and thesis statement. This should include where you will get your sources for your literature review, how many sources, and what kind of review of the sources you will do (i.e., what you're trying to extract from the research).
- Create a time-line for the completion of the paper from start to finish. (For example: By the end of week 5, I will have my three of my sources found and one of them annotated; by the end of week 6, I will have two more sources and annotated four of them; by the end of week 7, I will have completed my outline and annotated bibliography.)
- Refer to the headings and guidelines for the sections to be covered in your final paper.

Progress Report

- Identify which of the case studies provided you will be using for your Security Research Paper.
- Write a methodology and thesis statement. This should include where you'll get your sources for your literature review, how many sources, and what kind of review of the sources you will do (i.e., what you're trying to extract from the research).
- Refer to the headings and guidelines for the sections to be covered in your final paper.

Final Report

Formulate and write the paper using the following headings and guidelines (they don't have to be exactly matched but highly encouraged).

1) Introduction to Serverless Computing
   a) Provide background on Serverless computing
2) Serverless Computing Providers (comparison)
   a) Identify the improvement from Serverful computing from a Software Quality Point of View.
3) Compare and contrast different providers.
   a) General Security Issues in Serverless and Serverful Computing Environment
   b) Compare and contrast the benefits and drawbacks between different Serverless Computing Services in defenses to the vulnerability.
   c) Any Security Services to Cloud Architecture such as Application layer transport security in Cloud
4) Security Measures or Remedies Available in Serverless Computing
   a) (e.g.) Authentication and Authorization Models in Various Providers
   b) Access Management, Logging or Monitor Services, Encryption, etc.
   c) Any limitations exposed.
5) Conclusion

a) Choose and describe which remedy(s) or defense(s) should be adopted for a particular situation and why based on your analysis and professional or academic sources in Serverless computing.
b) Future of Security Measures in Serverless Computing.

TP Report

The student will provide a report formatted based on a template provided by the instructor. Students are required to improve the writing iteratively and incrementally every week. The revision will always happen during a quarter. Students will add new required sections to the existing paper every week.

The final report is the culmination of applied research and activities conducted throughout the quarter. The final report/paper provides a detailed problem and its solution likely to be encountered by a company or organization described in a case study supplied by the student.

Rubric for TP01 and TP02

Criteria	***% of Grade***
Structure	20%
Content	30%
Writing	30%
Reference	10%
Collaboration	10%
TOTAL	100%

Rubric for TP03

	Criteria	***Outcome***	***% of Grade***
Secure Systems & Programs Principles and Practices (20%)			
1	Secure Systems and Programs	Apply concepts, integration, and management of key components of secure systems and programs.	20%
Critical Thinking (60%)			
2	Issue	Issue is stated and described thoroughly so that it is understood fully.	20%
3	Evidence	Information is taken from source(s) appropriate to the scope with enough interpretation and evaluation to develop a comprehensive analysis or synthesis, and expert opinions are thoroughly scrutinized.	10%
4	Context and Awareness	Thoroughly analyzes assumptions and biases, carefully evaluating contextual relevance when presenting a position.	20%

5	Conclusions	Conclusions are logical and reflect an informed evaluation of evidence and perspectives in priority order.	10%
Collaboration (20%)			
6	Teamwork	Works effectively on diverse, global and/or distributed teams.	10%
7	Knowledge of Cultural Frameworks	Demonstrates sophisticated understanding of the complexity of elements important to members of another culture in relation to its history, values, politics, communication styles, economy, or beliefs and practices.	5%
8	Openness to Cultural Differences	Demonstrates sophisticated understanding of the complexity of elements important to members of another culture in relation to its history, values, politics, communication styles, economy, or beliefs and practices.	5%
	TOTAL		100%

TP Presentation

The student will report the research outcomes, development, or other project efforts to an academically appropriate committee in a public forum. The nature of the presentation content will determine the specific makeup of the audience. The student will choose the format of the presentation in consultation with the advisor. The layout and design must be appropriate and adequate to represent the outcomes of the effort. While students must make some form of a visual presentation, the presentation of the results may include publishing in a refereed publication, publication in a trade or popular magazine or journal, broadcast in an appropriate medium, or, in exceptional cases, limited dissemination within a closed community.

Each presenter will have 15 minutes for presentation and 5 minutes for questions and answers. Each presenter must keep the total presentation time limit strictly.

Criteria	***% of Grade***
Structure	20%
Visual Presentation	30%
Verbal Quality & Engagement	30%
Collaboration	20%
TOTAL	100%

Course Policies

Course policies on topics such as *Late Assignments, Participation,* and *Professional Writing* are found under *Course Information* in the online course menu. Students are responsible for reviewing and applying these policies while enrolled in this course.

University Policies

Students are responsible for understanding and adhering to all of City University of Seattle's academic policies. The most current versions of these policies can be found in the University Catalog that is linked from the CityU Web site.

Antidiscrimination

City University of Seattle and its staff and faculty are committed to supporting our students. We value equity, diversity, and inclusion as a way of life as well as the educational opportunities it provides. City U will not tolerate any form of discrimination based on race, color, ethnicity, sexual orientation, gender identification, socioeconomic status, or religious values. If you have experienced any discrimination based on any of the above, we encourage you to report this to the University. Please report this to your instructor. If you do not feel safe reporting this to your instructor, please report to Dr. Scott Carnz, Provost or to the Vice President of Student Affairs, Melissa Mecham.

Non-Discrimination & Prohibition of Sexual Misconduct

City University of Seattle adheres to all federal, state, and local civil rights laws prohibiting discrimination in employment and education. The University is committed to ensuring that the education environment is bounded by standards of mutual respect and safety and is free from discriminatory practices.

In the U.S., the University is required by Title IX of the Education Amendments of 1972 to ensure that all of its education programs and activities do not discriminate on the basis of sex/gender. Sex include sex, sex stereotypes, gender identity, gender expression, sexual orientation, and pregnancy or parenting status. Sexual harassment, sexual assault, dating and domestic violence, and stalking are forms of sex discrimination, which are prohibited under Title IX and by City University of Seattle policy. City University of Seattle also prohibits retaliation against any person opposing discrimination or participating in any discrimination investigation or complaint process internal or external to the institution. Questions regarding Title IX, including its application and/or concerns about noncompliance, should be directed to the Title IX Coordinator. For a complete copy of the policy or for more information, visit https://my.cityu.edu/titleix or contact the Title IX Coordinator.

In Canada, in compliance with the British Columbia Human Rights Code, the Alberta Human Rights Act, WorksafeBC, and the Workers' Compensation Board of Alberta, the University believes that its environment should at all times be supportive and respectful of the dignity and self-esteem of individuals. Discrimination, harassment and bullying conduct, whether through person to person behaviour or via electronic communications such as email or social

media is not acceptable and will not be tolerated. As an educational institution, it is our responsibility to cultivate an environment of excellence, equity, mutual respect and to recognize the value and potential of every individual. The University will take all necessary steps to meet or exceed the requirements of the law to prevent discrimination, harassment and bullying. The Respectful Workplace Policy for the prevention of discrimination, harassment and bullying policy and procedure can be found at https://www.cityu.edu/discover-cityu/about-cityu/ under the Policies section or at https://www.cityuniversity.ca/about/ .

Title IX Statement

City University of Seattle and its faculty are committed to supporting our students and seeking an environment that is free of bias, discrimination, and harassment. If students have encountered any form of sexual misconduct (e.g. sexual assault, sexual harassment, stalking, domestic or dating violence), we encourage them to report this to the University. If a student speaks with a faculty member about an incident of misconduct, that faculty member must notify CityU's Title IX coordinator and share the basic fact of the experience. The Title IX coordinator will then be available to assist students in understanding all of the options and in connecting students with all possible resources on and off campus.

To view CityU's sexual misconduct policy and for resources, please visit the Title IX and Campus Safety pages in the my.cityu.edu portal.

Religious Accommodations

Washington state law requires that City University of Seattle develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The University's policy, including more information about how to request an accommodation, is available in the University Catalog. Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request Form found on the student dashboard in the my.cityu.edu student portal.

Academic Integrity

Academic integrity in students requires the pursuit of scholarly activity that is free from fraud, deception and unauthorized collaboration with other individuals. Students are responsible for understanding CityU's policy on academic integrity and adhering to its standards in meeting all course requirements. A complete copy of this policy can be found in the University Catalog under *Student Rights and Responsibilities* on the page titled *Academic Integrity Policy.*

Attendance

Students taking courses in any format at the University are expected to be diligent in their studies and to attend class regularly.

Regular class attendance is important in achieving learning outcomes in the course and may be a valid consideration in determining the final grade. For classes where a physical presence is

required, a student has attended if they are present at any time during the class session. For online classes, a student has attended if they have posted or submitted an assignment. A complete copy of this policy can be in the University Catalog under *Student Rights and Responsibilities* on the page titled *Attendance.*

Final Assignments Due Date

Final assignments for each class at CityU must be due on or before the final date of the course as indicated in the university's course information system. Due dates that extend beyond the final date of the course may negatively impact tuition funding for students.

Support Services

Disability Services Accommodations Statement

Students with a documented disability who wish to request academic accommodations are encouraged to contact Disability Support Services to discuss accommodation requests and eligibility requirements. Please contact Disability Support Services at *disability@cityu.edu* or 206.239.4752 or visit the Disability Support Services page in the my.cityu.edu portal. Confidentiality will be observed in all inquiries. Once approved, information about academic accommodations will be shared with course instructors.

Library Services

CityU librarians are available to help students find the resources and information they need to succeed in this course. Contact a CityU librarian through the Ask a Librarian service, or access library resources and services online, 24 hours a day, seven days a week.

Smarthinking Tutoring

CityU students have access to free online tutoring offered through Smarthinking, including writing support, from certified tutors 24 hours a day, seven days a week.
Contact CityU's Student Support Center at help@cityu.ed to request a user name and password.