Engineering Privacy in Software
Course Numbers: 17735, 19605, & 95878

Dr. Timothy Libert (`timlibert@cmu.edu`)

Spring 2020

Office Hours: Thursday 2-4pm	Class Hours: MW 12 - 1:20 PM
Office: 2125, Collaborative Innovation Center	Class Room: GHC 4101

Course Description

Privacy harms that involve personal data can often be traced back to software design failures, which can be prevented through sound engineering practices. In this course, students will learn how to identify privacy threats due to surveillance activities that enhance modern information systems, including location tracking, behavioral profiling, recommender systems, and social networking. Students will learn to analyze systems to identify the core operating principles and technical means that introduce privacy threats, and they will learn to evaluate and mitigate privacy risks to individuals by investigating system design alternatives. Strategies to mitigating privacy risk will be based on emerging standards and reliable privacy preference data. Students will have the opportunity to study web-, mobile- and cyber-physical systems across a range of domains, including advertising, healthcare, law enforcement and social networking. In addition, students will know how, and when, to interface with relevant stakeholders, including legal, marketing and other developers in order to align software design with privacy policy and law.

The course format has four main components: first, class lectures, guests speakers, and readings will introduce you to core concepts in privacy engineering; second, you will produce several threat reports whereby you will find and analyze examples where real-world systems and products have failed to protect privacy; third, a semester-long group assignment will develop a functional software system designed to protect user privacy; fourth, discussion and deliberation will provide an environment in which to present your threat reports, refine your own project ideas, and provide feedback to your classmates. For these reasons, attendance is required and your grade will depend on the quality of your project outputs and deliberative contributions.

Learning Objectives

After completing this course students will gain an understanding of:

1. The Need for Privacy Engineering
    - Foundational concepts in privacy
    - Differences between privacy by policy and privacy by architecture
    - Regulatory requirements for privacy by design
2. Privacy Engineering on the Web
    - Fundamentals of web architecture
    - Fundamentals of authentication on the web
    - Common privacy issues on the web
3. User Privacy Concerns
    - Identify privacy risks emerging from software system design
    - Analyze the unique privacy concerns of sensitive groups
    - Use personas and goals to develop software requirements
4. Privacy-Focused Software Development Processes
    - Utilize Privacy by Design strategies
    - Design subject access request systems
    - Implement privacy-protective data storage techniques
    - Conduct privacy impact assessments
5. Current Challenges in Privacy Engineering
    - Identify privacy risks arising from personalization and localization
    - Identify privacy risks arising from tracking and surveillance
    - Analyze challenges to managing consent and privacy preferences

Prerequisites

There are no formal prerequisites for this course but students should be able to read complex texts and are expected to have either programming or project management experience.

Required Readings

There is no single text book: readings will be a mix of academic articles, book chapters, and online resources. All readings will be posted to Canvas.

Course Requirements and Grading

- **5%** Attendance
- **15%** Participation
- **20%** Threat Reports
- **60%** Group Project

Attendance

Attendance forms 5% of the grade and is required, but over the course of the semester you get two "free passes" by which you may miss class with no explanation needed provided you notify instructors prior to 9 AM. These free passes do not apply to days you or your team are scheduled to present, and missing more than two classes will require relevant documentation of your inability to make class, such as a doctors note.

Participation

Participation forms 15% of your grade and everybody is expected to speak on a regular basis. You will be graded along the following dimensions:

- Asking questions during lecture
- Presenting your ideas and progress to the class during discussion
- Giving thoughtful feedback to your classmates and contributing to dialogue
- Referring to class readings to support arguments you make in discussion

Threat Reports

Over the course of the semester you will submit and present three analyses of privacy threats covered in the popular press. These threat reports will constitute 20% of your grade. The details of the threat reports are described in an additional document and on Canvas.

Group Project

The biggest portion of your grade (60%) is determined by a semester-long group project. This project will require you to research the needs and privacy concerns of an at-risk group and develop a software tool which helps them solve a problem in a privacy-preserving way. Several milestones over the course of the semester will help you with your progress. The details of the project are described in an additional document and on Canvas.

Course Schedule

Date	Lecture Topic	Assignment Due
1/13/20	Course Intro	
1/15/20	Foundational Privacy Concepts	
1/20/20	No Class, MLK	
1/22/20	Privacy by Policy & Architecture	Work Organization Plan
1/27/20	Web Architecture	
1/29/20	Refugees (*Kate Coyer, Harvard / CEU*)	Threat Report 1
2/3/20	Web Authentication	
2/5/20	Children (*Jennifer Sydeski Hurd, Connect Wolf*)	To-Do Web App
2/10/20	Privacy Problems on the Web	
2/12/20	Partner Violence (Guest TBA)	Web App Authentication
2/17/20	User Personas and Goals	
2/19/20	Proposal Presentations	Project Proposal
2/24/20	Privacy by Design Strategies	
2/26/20	Threat Report 2 Presentations	Peer Review 1, Threat Report 2
3/2/20	Subject Access Requests	
3/4/20	Requirements Presentations	Project Requirements
3/9/20	No Class, Spring Break	
3/11/20	No Class, Spring Break	
3/16/20	Privacy Risk Analysis	
3/18/20	Progress Presentations	Revised Requirements
3/23/20	Privacy Impact Assessments	
3/25/20	Progress Presentations	
3/30/20	Legal Requirements for Privacy Engineering	Threat Report 3
4/1/20	Threat Report 3 Presentations	
4/6/20	Data Anonymization	
4/8/20	Prototype 1 Demo Presentation	Prototype 1
4/13/20	Discrimination and Bias	
4/15/20	Progress Presentations	
4/20/20	Surveillance	
4/22/20	Progress Presentations	
4/27/20	TBD	Prototype 2
4/29/20	Final Presentations / Demo	
5/1/20		Final Report + Code

Course Policies

Late Work

For individual assignments you are allowed to turn in one assignment up to 24 hours late without penalty provided you notify instructors 24 hours early in advance (eg. if the assignment is due Monday at 5pm you must notify us by Sunday at 5pm that you will turn it in before Tuesday at 5pm). The same policy applies to one group milestone provided it does not impact a presentation day. Otherwise, late work over 24 hours will receive at most half credit and late work over 48 hours will receive no credit. Exceptions may be made if you provide relevant documentation of your inability to turn in your work, such as a doctors note.

Screen Policy

This course will be a mix of lecture and discussion. Laptops will be allowed on days we have lectures, but on not on days we have guests or discussions. This is for three main reasons: first, laptops can be distracting to yourself and others; second, it is rude to guest speakers for students to be on laptops; and third, given 20% of your grade depends on participation you need to be engaged with your classmates and not your social media feeds. Smartphones are never allowed in class.

Academic Integrity

Copying other people's work without attribution, be it written work or software, will not be tolerated. When you use the work or ideas of others you must provide relevant citations. This includes referring to popular press articles, academic articles, books, and software (including open-source libraries). Violations will be handled in accordance with Carnegie Mellon's Academic Integrity policy: http://www.cmu.edu/policies/student-and-student-life/academic-integrity.html.

Learning Accommodations

If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources at getchell@cmu.edu or 412-268-6121. If you have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.

Take care of yourself

This course is important, but not as important as your personal health and well-being. Do your best to maintain a healthy lifestyle this semester by eating well, exercising, moderating your use of drugs and alcohol, getting enough sleep, and taking time to relax. Taking breaks and spending time with friends will refresh your mind and give you new perspectives on your work, allowing you to do a better job.

If you or anyone you know experiences any academic stress, difficult life events, or difficult feelings like anxiety or depression, we strongly encourage you to seek support. Consider reaching out to a friend, faculty, or family member you trust for assistance. Likewise, CMU's

Counseling and Psychological Services (CaPS) is a mental-health resource used by over 25% of students during their time at CMU. CaPS may be reached by calling 412-268-2922 or visiting their website: http://www.cmu.edu/counseling/

If you or someone you know is feeling suicidal, call someone immediately, day or night:

- CaPS: 412-268-2922
- Resolve Crisis Network: 888-796-8226
- If the situation is life threatening, call the Police:
  - On campus: CMU Police: 412-268-2323; Off campus: 911