CPS 586: Usable Security & Privacy
Spring 2024

Last Updated on January 29, 2024

1 General Course Information

Course Title: Usable Security and Privacy

Class Location: Gross Hall 103

Class Time: Mondays and Wednesdays at 4:40 p.m. - 5:55 p.m.

Course Schedule: https://tinyurl.com/5xpvx8df

Course Website: https://courses.cs.duke.edu/spring24/compsci586/

Course Canvas: https://canvas.duke.edu/courses/27440

Course Ed: https://edstem.org/us/courses/50166/discussion/

Class Recordings: http://tinyurl.com/38jmb5xd

Course Instructor Office Hours: Wednesdays at 5:55 (right after the class). If this time slot does not work for you, please email me to schedule a different time to chat.

Course Instructor Office Hours Location: Gross Hall 103

Course Instructor: Pardis Emami-Naeini (she/her) - pardis@cs.duke.edu

Course Teaching Assistant: Wanyi Chen (she/her) - wanyi.chen503@duke.edu

2 Course Description

Security and privacy problems are societal challenges that technology cannot solve. The increasing security and privacy incidents, including phishing, identity thefts, and attacks on consumer smart devices, highlight the growing need to establish a continuous and in-depth understanding of users' critical and undeniable role in these situations. This course will introduce several security and privacy topics that have a strong human factors component.

Students will learn user research methods to effectively study people's security and privacy attitudes, concerns, and practices when interacting with technologies. Below are some of the themes that we will cover throughout this course:

- User Research Methods and Ethics
- Equity and Inclusivity in Security and Privacy

- Developing Usable Security and Privacy Tools
- Security and Privacy Education and Awareness
- Human-Centered Security and Privacy in Emerging Technologies

This course is suitable both for students who are interested in security and privacy and would like to learn more about the role and importance of human factors and usability in cybersecurity, as well as those who are interested in usability and human-computer interaction (HCI) and are eager to know more about how fundamentals of HCI can be applied to improve people's security and privacy. Although there are no hard requirements, the course is most suitable for students who have some programming background (e.g., an undergraduate computer programming course).

This course includes weekly reading commentaries, a midterm exam, and a final user-centered research project. The reading assignments are designed to introduce students to a variety of research topics in human-centered security and privacy and encourage them to critically examine usable security and privacy projects and ideas. For the final research project, students will work in small groups and deliver project status updates as well as a final report. Those who are interested will have a potential mentorship opportunity to extend their user research and publish a full paper or a poster at a top-tier venue in HCI (e.g., CHI, CSCW), privacy and security (e.g., USENIX Security, IEEE S&P), or usable privacy and security (e.g., SOUPS).

3 Course Structure

At a high level, this course follows the structure below:

- **Class Lectures (see Section 9):** Through several short lectures, I will be teaching the core topics in usable and human-centered security and privacy. These topics are designed to teach you the principles of conducting research and practice related to inclusive security and privacy.
- **Reading Commentaries (see Section 6):** There are two required readings for most sessions. These readings are selected to show students the range of topics in human-centered security and privacy research. These reading articles are extensively peer-reviewed and are published at flagship security, privacy, and HCI venues. The hope is that students can use the lessons learned from these readings to further strengthen their course projects. The complete list of readings is available on the course schedule. For most sessions, you are expected to read and submit a thoughtful commentary on the two readings assigned to the sessions. In each session of the class where we have reading assignments, one (or two) of your classmates will lead a discussion ($\sim$30 minutes) on the two readings ($\sim$15 minutes each). The deadline for submitting the commentaries of each class is 7 p.m. the day before that session.
- **In-Class Discussion (see Section 7):** Depending on the number of students enrolled in the class, each student is expected to sign up to lead the discussion for the readings of one or two sessions. This discussion should be around 30 minutes, and it should be structured in a way that a portion of it covers one reading and the second portion covers the second reading. If you are the discussion lead of a reading, you are not expected to submit the reading commentary for that specific reading; however, you are expected to submit the commentary for the reading you are not leading in that session. In addition, you should submit your presentation slides by 10 p.m. the night before the session, allowing the instructor to provide feedback on your slides before the class.
- **Class Project (see Section 8):** Throughout the course, you will work in small groups to conduct a research project in usable security and privacy. Since this class is cross-listed between different disciplines, you will probably work with students with diverse areas of expertise. You have the option to choose from a list of projects or propose a new project idea.

- **Midterm:** We will have a written midterm exam, where you are asked about the initial definitions of privacy, security, and usability. In addition, you will be asked questions related to the methodology of user-centered research.

4 Course Expectations and Goals

We work together to achieve the following objectives in this course:

- Learning about the importance of human factors and inclusivity in computer security and privacy.
- Getting exposed to the current topics in usable security and privacy research.
- Learning how to design appropriate human-centered usability studies.
- Learning quantitative and qualitative methods to analyze data collected from usability studies.

5 General Course Grading

Your final grade will be calculated based on the following rubric. Where needed, more detailed information about grading is provided in the rest of the syllabus.

- **Reading Commentaries:** 10% (see Section 6.3)
- **Discussion Lead:** 10% (see Section 7.2)
- **Active Class Participation:** 20%
- **Midterm:** 20%
- **Group Research Project:** 40% (see Section 8.1)

6 Reading Commentaries

Most lectures have two associated readings that are closely related to the topic of that session, either in terms of the topic or the research methods. For each session of the class (we have two sessions per week), you are expected to read and submit a thoughtful commentary on the two assigned readings. In each session of the class where we have reading assignments, one or two of your classmates will lead a discussion (∼30 minutes) on the two readings (∼15 minutes each). If you are assigned as a discussion lead of a reading, you are not expected to submit your commentaries for that reading. However, you are expected to submit your commentaries for the reading you are not leading its discussion in that session. For other students, the deadline for submitting the commentaries of each class is at 7 p.m. the day before that session.

The complete list of readings is available on the course schedule. If, as a discussion lead, you prefer to present a different article for your selected topic, you need to notify the instructor **at least one week** before the date of the session you are leading. The lead-selected articles should present peer-reviewed user-centered research on human-centered security. The article should be a full-length paper from any of the flagship security, privacy, or HCI conferences, including USENIX Security, IEEE S&P, PETS, CHI, HRI, and CSCW.

6.1 Expected Content of Commentaries

Please include the following items when preparing the commentaries for each assigned reading:

- Short summary (2-4 sentences) of the reading.
- Two discussion prompts (see Section 6.2).

6.2 Discussion Prompts

An important part of your reading commentaries is the discussion prompts. You are asked to write two discussion prompts per reading (four in total for each class) in your commentaries. These prompts can take a question or statement form. Regardless of how you format these prompts, they should demonstrate a deep understanding and critical thinking of the paper. Although there is no preferred type of prompt, below are a few questions that might inspire you when designing your prompts:

- What system design/user research methods are used in this research, are they effective (why/why not), and how can they be improved?
- Who could this research benefit or harm (e.g., consumers, policymakers) and why? What needs to be done to mitigate the potential harms of this research and/or strengthen its benefits?
- What are the risks of this research for study participants? Are there any unaddressed ethical concerns in this work?
- What lessons can we learn from this research, and what future directions can we think of that are inspired by this research?
- How has this work changed your understanding and view of security/privacy/human-computer interaction/usability?

6.3 Grading of Commentaries

For each class, you will receive two grades, one for each reading commentary. The assigned grade for your submitted reading commentary will be one of the following:

- **Complete Plus:** The commentary is detailed, and the included prompts demonstrate a deep understanding of the intellectual content of the reading. Each Complete Plus is an extra 0.25 points.
- **Complete:** The commentary is sufficiently detailed, and the included prompts demonstrate a sufficient understanding of the intellectual content of the reading.
- **Incomplete:** The commentary either lacks the expected components (see Section 6.1) or provides incorrect, incomplete, or shallow details about the reading. Each Incomplete is minus 0.25 points.

Your two lowest reading grades will be dropped. There is no deadline extension policy for reading assignments, and they are expected to be submitted by 7 p.m. the day before the class. However, life is full of surprises, which requires flexibility. So if, for any reason, you find it challenging to submit your assignments in time, please reach out to the instructor to discuss possible accommodations. Your health and happiness are my most important goals, so if you are in distress about this class (or anything else) and you would like to talk about it, the instructor is always available to chat. Just let me know!

7 In-Class Discussion

Depending on the number of students enrolled in the class, each student is expected to sign up to lead a class discussion for one or two readings. This discussion should be around 30 minutes, and it should be structured in a way that a portion of it covers one reading and the second portion covers the second reading. If you are the lead of one of the readings in a session, you are not expected to submit the commentaries for that reading. However, you are expected to submit the commentaries for the other reading which you are not leading in the session. Additionally, you should submit your presentation slides by 10 p.m. the night before the session, which would allow me to provide feedback on your slides before the class.

7.1 Discussion Strategies

Below are some potentially helpful practices you can consider when structuring your discussion strategies:

- **Reading Summarization:** Start the discussion by briefly summarizing the readings. Each student in the class is expected to read the articles and submit their commentaries prior to the class. Therefore, as a discussion lead, you do not need to spend a lot of time summarizing the details of the readings. However, to remind the class about the readings and keep the class on the same page, it would be helpful to start by providing a summary of the critical aspects of the readings. Your summary could include the goals of the reading, their methodology, and their main contributions. If there are points in the readings that you would refer to in the rest of the discussion, make sure to explain them clearly in your summary.
- **Class Participation:** As the discussion lead, you are the instructor of that discussion/reading. Therefore, you are expected to get students to talk and participate in the discussion. You will have access to students' commentaries, and you are encouraged to read through them to get inspired by some discussion prompts. If you are using some of the ideas from the students' prompts, it is a nice and good practice to credit the student who came up with that prompt. We all want to be acknowledged! :) To keep the conversation flow going, you can design some in-class activities. You might decide to break students into small groups so they can discuss among themselves for a few minutes and then inform the class about their conversations. This is just one idea, but it is up to you what in-class activities you would like to have.
- **Embrace the Teaching and Have Fun with it:** Above all, you are the teacher of the discussion. You are expected to view this teaching time not as a monologue but rather as an active engagement with your class. It is super important to have fun with your role and help students feel comfortable and included in the discussions and activities.

7.2 Discussion Lead Grading

As a discussion lead, you do not have to submit reading commentaries for the session that you are leading. Indeed, your reading grade for that session will be thoroughly based on your role as the discussion lead. I will consider the following criteria when assigning your reading grade:

- **Professional:** The slides are well-designed and presented. The discussion has an energetic flow, where most (if not all) students are actively engaged in it. The students' submitted commentaries were integrated into the presentation. The raised questions and comments in the discussion reflect a deep understanding of the readings and inspire new insights and perspectives on the readings. Each Professional is an extra 0.25 points.
- **Adequate:** The slides are in good shape and are understandable. The discussion questions/prompts help flow the conversation but do not excite all (most) students into actively participating in the

class discussion and designed activities. The students' submitted commentaries are integrated into a surface-level form without engaging with the questions in the discussion. The questions and insights raised are straightforward and do not reflect a deep understanding of the papers or critical thinking of the readings.

- **Insufficient:** The slides are not thoroughly readable/understandable. Either no meaningful discussion questions/prompts are raised in the class, or they are not helpful to help the conversation flow. The students' submitted commentaries are not integrated into the discussion. The discussion drifts without a well-designed structure, or the structure introduces a lot of dead time during the discussion. Each Insufficient is minus 0.25 points.

8 Course Research Projects

Throughout the course, you will work in small groups to conduct a research project on usable security and privacy. Since this class is cross-listed between different disciplines, you will probably work with students with diverse areas of expertise. You have the option to choose from a list of projects. If you have ideas for a topic that is not on the proposed list, you should first discuss the project idea with me by January 24. With your group, you will write a research paper on the project, and you will also present it to the class. In addition, you have an interim presentation where you have the opportunity to get feedback on your project prior to the final project presentation. The presenter of the interim project presentation should be different than the presenter of the final project presentation to make sure that more than one group member has the opportunity to share the exciting work you have done for the class.

To help you find a project, I will provide some suggestions on the topics and themes that you can choose from (see Section 8.2). These suggestions will be general topics, and you are expected to find important and feasible research questions that you would like to explore in the semester. Although not necessary, the project could entail designing a system prototype (e.g., interface, app, plugin), which should then be evaluated through user studies as part of the project. You may decide not to design a system and instead conduct empirical research on a usable security and privacy topic by collecting user data and then conducting appropriate analysis. If your proposed project includes a system design, the user study component of the project will be smaller compared to the projects with no system design. Regardless, all projects should have a user study component, either as its main contribution or a side contribution.

Students are encouraged to submit their research as a full paper or a poster to human-computer interaction (e.g., CHI, CSCW), security, and privacy (e.g., IEEE S&P, USENIX), or a usable security (e.g., SOUPS) venue. Submitting a full paper to these venues requires additional work beyond the semester. I will mentor students who are interested in continuing with their research projects and submitting them to the appropriate venues.

8.1 Project Timeline and Grading

Below is the tentative timeline for various stages of the project. The percentage of project grade for each item is provided in parentheses, if applicable:

- If you would like to propose project ideas that are not covered by the recommended list, you should discuss your proposal with me no later than January 30 at noon.
- Returning the project preferences form by February 1 at 7 p.m. You will then be assigned to a project team by February 5. (5%)
- Submitting a brief project proposal with your team by 7 p.m. on February 18. (5%)
- Giving a 4- to 6-minute project pitch. Slides are due by 10 p.m. on February 18. (5%)

- Finishing the required CITI training and sending the training completion certificate along with the IRB application draft to me by 7 p.m. on February 25 to get feedback. You should add my name as the PI. The complete IRB application should be submitted by March 1. (5%)
- Submitting a short interim project progress report by 7 p.m. on March 17. (5%)
- Giving a 6- to 8-minute recorded presentation on interim project progress. Slides are due by 10 p.m. on March 17. (5%)
- Giving a 10- to 12-minute final project presentation. Slides are due by 10 p.m. on April 14 or April 16. (20%)
- Submitting the final project paper by 7 p.m. on April 21. (50%)

8.2 Project Recommendations

Below are a few recommendations on the topic or theme of the research projects. If a theme looks exciting, you should work on defining a concrete research goal/question that you would like to explore in this course:

- Inclusive privacy and security by considering various user communities (e.g., demographics, accessibility).
- Privacy and security concerns/practices in smart homes.
- Privacy and security attitudes/practices of household members toward smart home devices.
- Usability of phishing warnings and users' nudging.
- Privacy and security concerns and practices in the gaming context.
- Dark/manipulative patterns in voice and video interfaces.
- Informing consumers' security and privacy purchase decision-making (e.g., apps, smart devices).
- People's understanding of smart device security and data practices.
- Concerns toward smart home devices in remote work settings.
- Concerns toward smart devices in academic settings.
- Security and privacy concerns, attitudes, and expectations toward augmented reality.
- Shared security and privacy practices and misconceptions on social media during the time of crisis (e.g., the war in Ukraine, demonstrations in Iran).
- Security and privacy concerns and attitudes toward popular categories of apps, including online dating apps, health apps, and educational apps.
- People's security and privacy risk perception and privacy attitudes toward large language models (LLMs) and/or AI-powered technologies.

9 Course Schedule

The course schedule can be found using this link: https://tinyurl.com/5xpvx8df. I will do my best to keep the schedule and the syllabus document unchanged during the semester. Any further changes to the schedule will be announced to all enrolled students in a timely manner.

10 Class and Collaboration Policies

Students are expected to follow the specified deadlines. However, I try to be as flexible as possible. If you need any special accommodations, please let the instructor know, and I will do my best to provide the help you need.

Students are allowed to discuss the readings among themselves. However, each student is responsible for writing the reading commentaries by themselves. Any collaboration on the midterm exam is strictly prohibited unless otherwise indicated by the instructor. Students are allowed to collaborate on the research project only among their group members.

11 Academic Integrity

We expect everyone to uphold the Duke Community Standard, which you can find here: https://gradschool.duke.edu/policies-forms/standards-conduct/duke-community-standard/. The standard is composed of the three following components:

- I will not lie, cheat, or steal in my academic endeavors;
- I will conduct myself honorably in all my endeavors and
- I will act if the Standard is compromised.

Please ask the instructor if there is any situation where you are not sure how to best comply with the specified components.

12 Inclusivity and Diversity

We are a diverse community, and we should work together to create an inclusive and welcoming environment for all students. We expect each member of this course (e.g., students, instructor, TAs) to make proactive efforts to make sure everyone feels comfortable in all aspects of the course, including class discussions and project participation. If you ever feel any discomfort for yourself or anybody else in this course, we ask you to raise your concern with the instructor if you feel comfortable sharing.

Duke University is committed to providing equal access to students with documented disabilities. Students with disabilities may contact the Student Disability Access Office (SDAO) to ensure their access to this course and to the program. There, you can engage in a confidential conversation about the process for requesting reasonable accommodations both in the classroom and in clinical settings. Students are encouraged to register with the SDAO as soon as they begin the program. Please note that accommodations are not provided retroactively. More information can be found using the following link: https://access.duke.edu/.

13 Anonymous Course Evaluation Surveys

No matter how many times I teach this course, there is always room for improvement, both in the content of the course and my teaching and mentorship. You are encouraged to talk to me/email me at any time to share your feedback. If you want to share your thoughts anonymously, I have created a short survey at the end of each session where you can provide your input. I am not collecting any personal information in this survey (e.g., demographics, IP address, location). Spending your time providing feedback is not always easy, but I will value each and every one of your inputs and greatly appreciate them all. :)

14 Taking Care of Your Health and Happiness

This course is important, but your continued health and happiness are far more valuable. More than anything, I expect you to take care of yourself by learning what works for you. For some of us, that means taking some time from our days for meditation, exercise, or talking to a therapist. The form of self-care is not important as long as you commit to it. I will try my best to be flexible, and I am always available to hear from you. So, if anything happens that you would like to share with me, please reach out. I am by no means a therapist, and you should always consider reaching out to licensed professionals, but the least I could do is listen, share my own (often wildly incomplete) view of things, and provide case-by-case accommodations if needed.

15 Acknowledgements

Parts of the course material and the syllabus have been inspired by, adapted from, or borrowed from the courses taught by wonderful mentors and colleagues, Lorrie Cranor, Blase Ur, Camille Cobb, Suavik Das, and Matthew Lentz.