CPS 586: Usable Security & Privacy
Spring 2026

Last Updated on January 5, 2026

1 General Course Information

Course Title: Usable Security and Privacy

Class Location: Wilkinson 132

Class Time: Wednesdays and Fridays at 1:25 p.m. - 2:40 p.m.

Course Schedule: https://tinyurl.com/3tdzbfwk

Course Website: https://courses.cs.duke.edu/spring26/compsci586/

Course Canvas: https://canvas.duke.edu/courses/73909

Course Ed: https://edstem.org/us/courses/91025/discussion

Class Recordings: https://tinyurl.com/exkh47ay

Student Hours: After the class on Wednesdays, or by appointment.

Course Instructor Student Hours Location: Wilkinson 132

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

Course Teaching Assistant: Jabari Kwesi (he/him) - jabari.kwesi@duke.edu

2 Course Description

Security and privacy problems are societal challenges that technical solutions alone cannot address. The increasing security and privacy incidents, including phishing, identity theft, 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 reading commentaries, a midterm exam, lab/in-class activities, 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:** Through several 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. See Section 8 for more details.
- **Reading Commentaries and In-Class Discussions:** For a subset of sessions, two required readings from top-tier security, privacy, or HCI venues will be chosen by the discussion lead(s). Leads and non-lead students have specific responsibilities regarding these sessions, which are discussed in Section 6.
- **Class Participation/Activities:** One of the most important components of this class is active class participation, which is different from class attendance. In addition to in-class questions and discussions, each session will include at least one class activity in which the instructor will ask students to work in small teams. Before leaving the session, students must submit or email their completed activity to the TA with their names included. As mentioned above, this component is different from class attendance. This means that if you do not attend a session, you can still receive the participation grade by watching the class recording and submitting your class activity no later than the beginning of the following session.
- **Class Project (see Section 7):** 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 6.1)
- **Discussion Lead:** 10% (see Section 6.2)
- **Active Class Participation:** 20%
- **Midterm:** 20%
- **Group Research Project:** 40% (see Section 7.1)

6 Reading Commentaries & In-Class Discussions

There will be two required readings for a subset of sessions, as marked in the class schedule. Each reading will be selected by the discussion leads (3–5 students) assigned to that reading. Assignments will be made through a survey in which students will be asked to specify their preferred sessions to lead. All students are expected to lead the discussion for one reading during the course. Half of each session ($\tilde{3}$0–35 minutes) will be dedicated to the first reading, and the other half will be dedicated to the second reading ($\tilde{3}$0–35 minutes).

The responsibilities of the discussion lead teams are to: (1) select a paper they are interested in leading the discussion on (latest by one week prior to their session). The paper should be a full-length article from any of the flagship security, privacy, or HCI conferences, including USENIX Security, IEEE S&P, SOUPS, PETS, CHI, HRI, and CSCW; (2) present a short summary of the paper's most important points ($\tilde{3}$–5 minutes); (3) lead an in-depth and lively discussion by proposing 1–2 discussion prompts (selected from prompts submitted by non-lead students) for small-group discussion in class ($\tilde{1}$0–15 minutes); and (4) design a short class activity related to the paper. This activity should involve the user research methods covered in the course (e.g., asking students to design a few survey questions related to a specific aspect of the paper, asking students to identify potential biases in interview questions used in the paper) ($\tilde{1}$0–15 minutes).

For each assigned reading, non-lead students are expected to submit an in-depth commentary demonstrating a clear understanding of the required reading (by 3 p.m. the day before the session). The TA will then share these prompts with the discussion leads (by 5 p.m. the day before the session), who will select a subset (1–2) to present to the class during their discussion. Students whose prompts are selected are expected to help initiate the discussion related to their prompts. Non-lead students are expected to have read the assigned papers in detail and to actively engage in these discussions. An example discussion prompt is: "The paper discusses the roles of designers and developers in ensuring AI safety. In your opinion, do policymakers have additional responsibilities in this area, and what might those responsibilities entail?"

In addition to the required readings, the teaching team has identified two optional readings that students may explore to deepen their understanding of the session's topic. Engaging with these supplementary materials may enhance students' understanding of the subject matter and provide broader perspectives. While not mandatory, reviewing these optional readings is encouraged for students interested in further exploration of the course content. The complete list of optional readings is available on the course schedule.

Digital Detox. In sessions with in-class discussions, we will have a digital detox. This means that students will be asked not to use any digital technologies, including phones, computers, and tablets, unless the activity designed by the discussion leads requires their use. Otherwise, the use of these technologies is not allowed in class. Students who need to use these tools for reasons unrelated to the class are asked to do so outside the classroom, to ensure that the discussion leads receive the attention they deserve for their awesome work leading the discussion. :)

6.1 Grading of Reading Commentaries

The assigned grade for your submitted reading commentary will be one of the following:

- **Complete:** The commentary is sufficiently detailed and demonstrates a sufficient understanding of the intellectual content of the reading. 1 point.
- **Incomplete:** The commentary provides incorrect, incomplete, or shallow details about the required reading. 0.25 points.

There is no deadline extension for reading commentaries, and they are expected to be submitted by 3 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 priorities, 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!

6.2 Discussion Lead Grading

As a discussion lead, you do not need to submit a reading commentary for the paper whose discussion you are leading. However, you are still required to submit a commentary for the second paper in the session, for which you are not leading the discussion. The following criteria will be used to evaluate your reading grade:

- **Complete:** 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 designed activities reflect a deep understanding of the readings as well as the user research methods taught in the class and inspire new insights and perspectives on the reading/methods. 1 point.
- **Incomplete:** No meaningful activities are developed and used in the class. 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. 0.25 points.

7 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 the instructor. With your group, you will write a research paper on the project, and you will also present it to the class. In addition, there will be at least two project check-in meetings with the instructor. The link to schedule the project check in: https://calendly.com/pardis-emami-naeini/research-chat-with-pardis-15-minutes.

To help you find a project, I created a list of themes/topics to select from (see Section 7.2). The list includes only general topics, and you are expected to find important and feasible research questions that you would like to explore in the semester within these topics (or new ones upon the instructor's approval). 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. 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.

7.1 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 the instructor no later than January 22.
- Returning the project preferences form by January 26 at 7 p.m. You will then be assigned to a project team by January 27. (5%)
- Completing the first 15-minute check-in meeting by February 9. (5%)
- Submitting a brief project proposal with your team by 7 p.m. on February 12. (5%)
- Giving a project pitch. Slides are due by 7 p.m. on February 12. (10%)
- Completing the second 15-minute check-in meeting by March 6. (5%)
- Giving a final project presentation on April 8 or April 10. Slides are due by 7 p.m. on April 7 or April 9, depending on your assigned presentation date. (20%)
- Submitting the final project paper by 7 p.m. on April 17. (50%)

7.2 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.

8 Course Schedule

The course schedule can be found using this link: https://tinyurl.com/mur7558k. 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.

9 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.

10 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.

11 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/.

12 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. :)

13 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.

14 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.