Project Scope

You are tasked with designing **a web-based communication system** to support university students doing **group work** (e.g., assignments and projects). Your design should go *beyond existing tools* like Slack, Discord, or Teams by focusing on the unique needs of students and their group work.

In the first phase, you will follow a *User-Centered Design (UCD)* process to **identify user requirements**, **design alternatives**, and **develop *lo-fi* prototypes**. Then, you will use a selected set of Large Language Models (LLMs) to assist in **developing *hi-fi* prototypes**. You will create an **evaluation plan** to see how they meet the design requirements.

In the second phase, you will define **security requirements** for your system. You will **evaluate vulnerabilities** in the generated system and apply **security solutions** to address them.

Things to note:

- The project is divided into two (2) phases, and each phase has a specific assignment that you have to submit on Canvas. Phases are designed so that you can chronologically follow them with overlaps.
- This is a group project. There should be 4 students per group, and where an exception can be made, groups of 3 students are allowed. You must make a case to your tutor why it has to be a group of 3. All the group members must be from the same tutorial group. Once you form the group, inform your tutor of the members of your group; they will set up your group in Canvas.
- We highly encourage you to include a reasonable overlap between the execution of project phases.
- We highly encourage you to use modern development tools (e.g., AI-assisted IDEs like Cursor or Windsuf) to minimize overhead, allowing you to focus on usability and security concepts.
- Keep all of your answers concise and on-point, and do not repeat yourself.
- We highly encourage you to develop the report concurrently while working on the project tasks, rather than starting the report after all the tasks are completed.
- The submission must be made in PDF format. All submitted *text* (report, codes, etc.) must be in *text* format that is readable by Turnitin. Do not convert the text part of the report to images (e.g., jpeg). If you submit in such a format, we may ask you to resubmit the report, and you may be subjected to late submission penalties. Please read the **Adobe PDF** section of the Turnitin file requirements section to see how you can ensure it is readable. The images in your report (e.g., images of your prototype) do not need to meet this requirement. LaTeX generated PDF files naturally meet this requirement unless you further process them.
- Every project member should contribute equally to the project (both the project tasks and writing the report) and **individual contributions should be reflected using the diary section of the report (Page 9)**. All the project-related code should be managed through the USyd Github.
- **Report Template:** The template for the report should follow the ACM CHI Publication Format (Links below). We highly recommend using Overleaf shared among the group. All the project members' names, SIDs, project group name (as it appear in Canvas) should be included as the author information. Submit the non-anonymised version. Incorrect template will incur penalties (-4pts per phase).
  - LaTeX in Overleaf
  - Microsoft Word

Phase 1 - Requirement Gathering & Design (100pts [weight 10%])

In this phase, you are required to develop the user requirements, concept and prototypes for your group project. This involves several tasks, as outlined below. Each task should be recorded in the report as a section and each sub-task as sub-sections. The total length of the Phase 1 report should not exceed 3000 words (excluding images, appendices and diary). Also, include the *diary* for the period as outlined on Page 9 at the end of the report.

Tasks:

1. Identify user requirements for the project. ***- Task total 50pts***

   (a) Develop a plan for a semi-structured interview to gather requirements for the proposed project. The plan must include: ***- 15pts***

   - The goal and a brief description of the study.
   - Who the potential participants are, along with inclusion/exclusion criteria. Groups of 4 must interview 4 participants, where groups of 3 - 3 participants. Participants must be recruited outside the INFO2222 (2025) cohort.
   - Study plan including planned activities, data to be collected, interview questions, data recording formats, and analysis plan.

   (b) Recruit participants and conduct the study. Include transcripts in the appendix. ***- 10pts***

   (c) Conduct a thematic analysis. Document the process followed and the results. ***- 10pts***

   (d) Using the themes as references, create a table of features required for your new system along with a short justification for each. Compare these to existing systems (Teams, Slack, etc.) and literature, and clearly outline if each feature exists in them. Cite the literature you refer to (use Google Scholar to search for related research works). We recommend you find at least 1-2 unique features matching the context of the project scope. ***- 5pts***

   (e) Write a *user scenario* of how your proposed project will be used. Please read these articles to learn about how to write a *user scenario*: [article 1, article 2] ***- 10pts***

2. Developing design alternatives. ***- Task total 25pts***

   (a) Follow the "10 plus 10 method" to sketch designs for a potential single-page web-based user interface to implement the system. As a group, select 3 designs per 4-student group or 2 designs per 3-student group. Please explain your ideas in the report (include your sketches). ***- 15pts***

   (b) Refine into a final design solution and justify it with your reasoning. Use the sketches from this design to develop a paper prototype. ***- 10pts***

3. Hi-Fi prototype and evaluation design. ***- Task total 25pts***

   (a) Use one of the AI-assisted IDEs (Cursor or Windsuf) to implement the selected design using appropriate prompts. The following considerations should be taken into account: ***- 15pts***

   - You should not use *DeepSeek* as the university suggests you not to.
   - You must clearly document all prompts and AI-generated content produced using AI-assisted tools as an appendix in your report, for reproducibility and to address plagiarism concerns. Any file, function, or substantial code snippet created or modified by AI assistance must be explicitly listed (see Table 1 for an example).
   - Please provide your source files (USyd Github link in the report) in your final submission.
   - Make sure the system has reasonable functionality (it is OK if not all the functions are working) at the live demo during the tutorial (Week 06). You must clearly indicate which functions do not work in the report.

- **[Important Note]**: In Phase 2, you will enhance your prototype with security features (authentication, encryption, secure transmission, etc.). Although this does not count toward your Phase 1 grade, you are encouraged to start considering these security aspects early if time permits.

(b) Develop a study plan for evaluating the Hi-Fi prototypes for usability using the Think Aloud) methodology. Please note that you do not have to conduct a study yet; you will be asked to conduct the study at the end of the project phase 2. The following considerations should take into account when revising: ***- 10pts***

- The goal and a brief description of the study.
- Who the potential participants are, along with inclusion/exclusion criteria. Groups of 4 must have 4 participants, whereas groups of 3 - 3 participants. You can recruit the participants from other groups so that you can conduct the study during tutorials (but all the participants can't be from the same group.)
- Study tasks. At least three concrete tasks per prototype should be evaluated.
- Pilot studies and ethical considerations (including required ethics documents). At least prepare the consent form from USyd - HREC.
- Study plan including planned activities, data to be collected, data recording formats, and analysis plan.

File Path	**Description**	**AI Tool**	**Prompt Used**
`hello.py`, `greeting.py`	Scripts printing greeting messages	claude-3.7-sonnet	"Write Python scripts that greet the user differently based on the time of day."
`README.md`	Basic project documentation	gpt-4o-mini	"Generate a short README file describing Python scripts that greet users based on the current time."

Table 1: Summary of AI-generated files and prompts used

Phase 2 - Security, Evaluation & Report (200pts [20%])

You will enhance the security of the group communication system built in Phase 1, demonstrate the impact of missing security measures, and evaluate the security awareness of Large Language Models (LLMs). The goal is to deepen your understanding of security vulnerabilities and defenses through hands-on implementation and analysis. You are encouraged to use modern development tools (e.g., AI-assisted IDEs like Cursor) to minimize overhead, allowing you to **focus on security features and concepts**.

Key objectives:

- *Task 1 (60 points):* Implement critical security features (e.g., authentication, encryption, secure transmission, certificate validation) and ensure their correct functionality.
- *Task 2 (60 points):* Conduct controlled experiments to demonstrate vulnerabilities arising from missing or misconfigured security measures, illustrating worst-case attack scenarios (e.g., man-in-the-middle, replay attacks, weak password storage).
- *Task 3 (80 points):* Assess and compare how different LLMs handle security-related queries, identifying their strengths, limitations, and potential biases in security advice.

Task 1 - Security Implementation - *Task total 60pts*

Enhance the communication system you developed in Phase 1, so that it ensures user authentication, message confidentiality, and integrity.

Submission Requirement:

- A **5-minute video** demonstrating your implementation.
- You must clearly document all prompts and AI-generated content produced using AI-assisted tools as an appendix in your report, for reproducibility and to address plagiarism concerns. Any file, function, or substantial code snippet created or modified by AI assistance must be explicitly listed (see Table 1 for an example).
- Please provide your source files (USyd Github link in the report) in your final submission.

Grading Criteria (based on recorded video and short Q&A in week 12's tutorial):

1. **Secure Password Storage**
   (a) Explain the characteristics of a strong hashing algorithm and justify your choice. ***- 10pts***
   (b) Implement a secure password hashing method with proper salting. Plaintext storage or weak hashing will result in deductions. ***- 10pts***
2. **Server Authentication on Login**
   (a) The client must verify the server's certificate before transmitting credentials. ***- 10pts***
   (b) If a hardcoded CA public key is used, discuss its security implications. Explain how the server certificate is generated (including the CA certificate). ***- 10pts***
3. **Secure Password Transmission**
   (a) Passwords must be transmitted over a secure channel (e.g., TLS 1.2+). Plaintext transmission of passwords is strictly prohibited. ***- 10pts***
4. **Secure Message Transmission**
   (a) Messages must be encrypted end-to-end (E2EE). ***- 10pts***

Task 2 - Security Demonstrations - *Task total 40pts*

Demonstrate at least **two distinct security vulnerabilities** by disabling or misconfiguring security features in your system. The goal is to illustrate the consequences of neglecting security best practices.

Submission Requirement:

- A **3-minute video** per vulnerability, demonstrating the attack. Clearly explain the attack, its impact, and how proper security measures mitigate it.
- You must clearly document all prompts and AI-generated content produced using AI-assisted tools as an appendix in your report, for reproducibility and to address plagiarism concerns. Any file, function, or substantial code snippet created or modified by AI assistance must be explicitly listed (see Table 1 for an example).
- Please provide your source files (USyd Github link in the report) in your final submission.

Grading Criteria (based on recorded video and short Q&A in week 12's tutorial):

1. **Vulnerability 1 Demonstration**
   - Present an attack scenario caused by disabling or misconfiguring a security feature. ***- 10pts***
   - Explain why the vulnerability occurs and how to fix it. ***- 10pts***
2. **Vulnerability 2 Demonstration**
   - Demonstrate a second, distinct attack scenario. ***- 10pts***
   - Explain why the vulnerability occurs and how to fix it. ***- 10pts***

Example Attack Scenarios (Choose at least one):

- **Message Interception:** Disable encryption or certificate validation to demonstrate eavesdropping via a network sniffer.
- **Weak Password Storage:** Store passwords in plaintext or use weak hashing (e.g., MD5, SHA-1) and demonstrate password retrieval by an attacker.
- **SQL Injection:** Exploit improper input handling to manipulate database queries.
- **Denial-of-Service (DoS):** Remove rate limiting and show how repeated requests degrade system performance.

Task 3 - Evaluation *- Task total 20pts*

1. Conduct the Think Aloud study planned at the end of the Phase 1. Groups of 4 must have at least 4 participants, whereas groups of 3 must have at least 3 participants. ***- 10pts***

2. Outline key findings as successful and unsuccessful tasks. Use these results to compare how different LLMs performed in terms of assuring usability in the web interfaces they generate. ***- 10pts***

Task 4 - (Research) LLM Security Awareness Evaluation - *Task total 80pts*

This task evaluates how well modern LLMs understand security concepts, assessing their biases and weaknesses in security-related advice. This is an open-ended **mini research** component, where you are encouraged to uncover novel insights about LLM security awareness.

Submission Requirement:

- A written report documenting your approach, key findings, and analysis.
- Focus on identifying **unexpected** or **previously unknown** behaviors in LLM responses.

Grading Criteria:

- Clearly explain your findings. ***- 10pts***
- Support your findings with quantitative data. ***- 10pts***
- Compare your findings to existing research or common beliefs. ***- 10pts***
- Demonstrate the novelty of your finding (Please read this blog post:). ***- 10pts***

Each investigation area is graded out of **40 points**, with a maximum of **80 points** for two distinct investation areas.

Suggested Investigation Areas:

- **Security Q&A with LLMs:** Evaluate LLM responses to security-related questions (e.g., secure coding, best practices). Assess their accuracy, completeness, and potential misinformation. Compare responses across models (e.g., ChatGPT, GPT-4, Google Bard, LLaMA-2).
- **Bias or Inconsistencies:** Investigate if LLMs consistently recommend secure practices or exhibit biases based on question wording, user persona, or context.
- **Adversarial Prompts / Jailbreaking:** Test whether LLMs can be manipulated into providing insecure responses. Explore adversarial prompts to assess their resilience to social engineering, prompt injection, or security policy bypasses.

Important:

- **Research novelty is key** – routine observations will not receive full marks.
- Keep explanations clear and concise.
- Cite relevant prior research where applicable.

Weekly Diary - All phases

You are required to submit a diary at the end of each project phase indicating the individual contributions you made to the project and the report. This should be a summary of your activities for each week. You should follow the following tabular format.

Group Name		
Week	**Student Name**	**Activities**
W03	Jane Doh	Joined the meeting to discuss ideas and contributed to ideation
W03	John Doh	Joined the meeting to discuss ideas and contributed to ideation
W04	Jane Doh	Drafted project scope
W04	John Doh	Made the listed of planned activities
W05	...	...