Computer Science Department, Purdue University
Fall 2023

Prof. Vassilis Zikas
Mohammad Hassan Ameri & Albert Yu

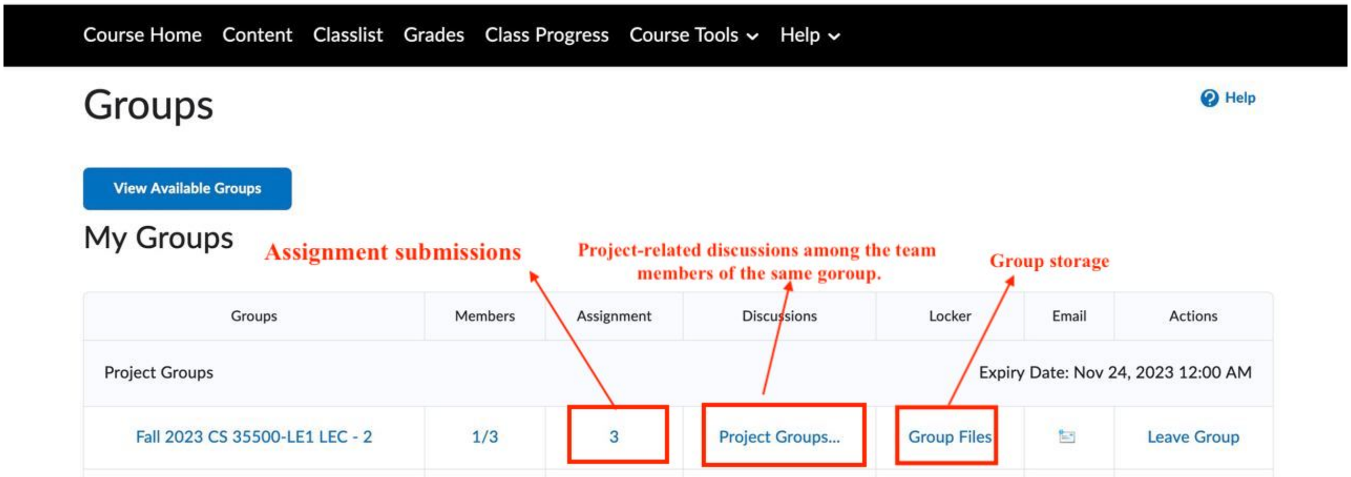
Project Handout

Due dates

- **Submit Team Roster and specifying coding language (over Gradescope):**
  Tuesday, November 17, 2023 23:59, EST
- **Code and Spec/Security Analysis Final Commit:**
  Wednesday, November 29, 2023 23:59, EST
- **Attack/Endorsement Submission:**
  Sunday, December 3, 2023 23:59, EST
- **Presentation In-class:**
  Tuesday December 5, 2023

1.1 Declare your team

You may form teams of up to 3 students. You may give your team a name. You can utilize Piazza post @5 to team up with other students. **When your group is finalized, submit a pdf file to Gradescope with each of the team member's name, and optional team name. You also need to specify the coding language you plan to use for implementation.** The instructor team will add your group members on Brightspace, where you can utilize group discussion page, group storage, and submit corresponding assignments (shown in the snapshot below).



Assignment submissions

Project-related discussions among the team members of the same gorоup.

Group storage

Groups	Members	Assignment	Discussions	Locker	Email	Actions
Project Groups						Expiry Date: Nov 24, 2023 12:00 AM
Fall 2023 CS 35500-LE1 LEC - 2	1/3	3	Project Groups...	Group Files		Leave Group

1.2 Set up

- Choose your language to implement the pseudo-code provided below. You may use any of the languages specified in the slides (c++, java, python, or rust) and make use of its cryptographic libraries.
- Create a private GitHub repository for your team.

1.3 Protocol specification

In your implementation, you need to have the following componnents. We just describe these function as the pseudo code for ease of your implementation.

- Communication: First of all you need to establish a communication environment to chat between the parties for exchanging the actual protocol-related messages between Alice and Bob. For example you can use socket programming to implement this part. The future exchanged messages are basically the ciphertext/signatures or MACs you may need in different phases of your protocol. So you need to make sure how to encode these cryptographic-related messages to send through the channel you are using.
- Protocol: This is the actual (potentially interactive) protocol that will be executed in order to perform the secure comparisson.

1.4 Code and spec / Security Analysis

Implement the functions in the **Protocol Specification**. By the final commit deadline you will need to submit (on Brightspace) a GitHub repository link, and the version number at the time of submission. Make the GitHub repository accessible to the instructors team (*will update the instructor GitHub accounts later*). The committed version should include a protocol specification, implementation, and security analysis, as below.

- Specifications of which language & libraries you used, etc.
- Security analysis of your team's encryption scheme. You should specify your security goals and show that they are achieved.

Any commit done to the the repo after that deadline will render the team disqualified. Please make sure your code compiles before submitting your code.

Electronic turn-in instructions:

1. Name your pdf document <`your group name`>`_code-spec.pdf`. Include GitHub repository url, and the version number at the time of submission in the pdf.
2. Your code or spec should not include de-anonymizing information (comments, author names, group-name etc).
3. Go to your group assignment in Brightspace & submit.

1.5 Attack/endorsement

We will announce the red-blue combinations on group discussion page on Brightspace once codes have been submitted. Your team will now act as red team and will be assigned two blue teams. You can attack or endorse each of the two blue teams. You may attack the theory (insufficient goals incorrect argument) or implementation (bugs, wrong libraries, low performance, etc).

Electronic turn-in instructions:

1. Name your pdf document <`your group name`>`_attack-endorse.pdf`.
2. Go to your group assignment in Brightspace & submit.

1.6 Presentation

There will be an in-class presentation. The duration of the presentation will be around 5 minutes. Include short description of your implementation, demo, attack (if applicable). Turn in your slides by midnight on Brightspace.

Electronic turn-in instructions:

1. Name your pdf document (of the presentation slides) <`your group name`>`_presentation.pdf`.
2. Go to your group assignment in Brightspace & submit.