IEMS5710 Individual Programming Lab Task in Python3

Daoyuan Wu

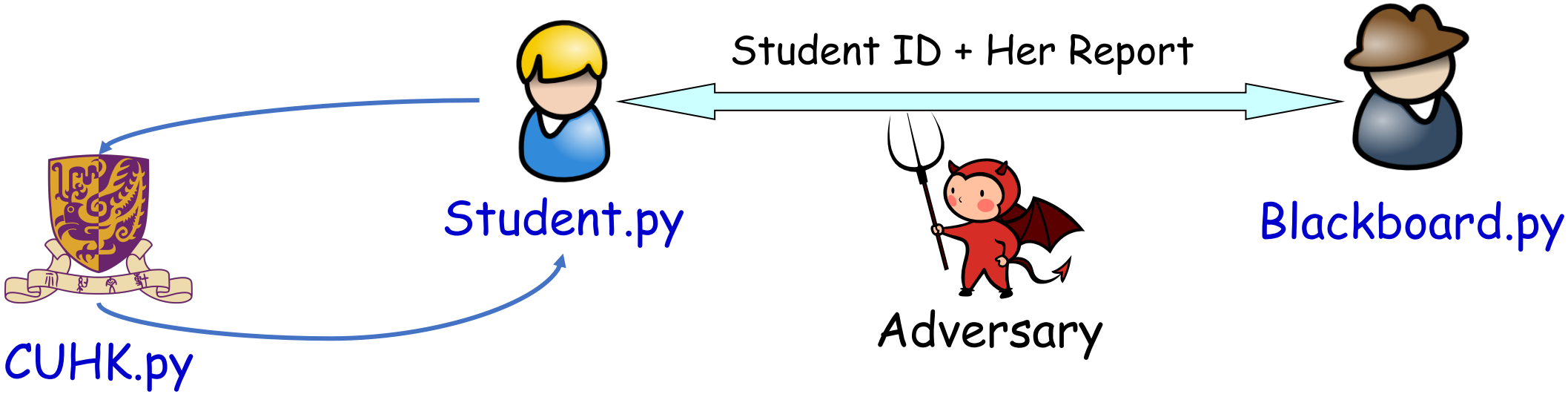
dywu@ie.cuhk.edu.hk

7 September 2022 (Updated on 12 October)

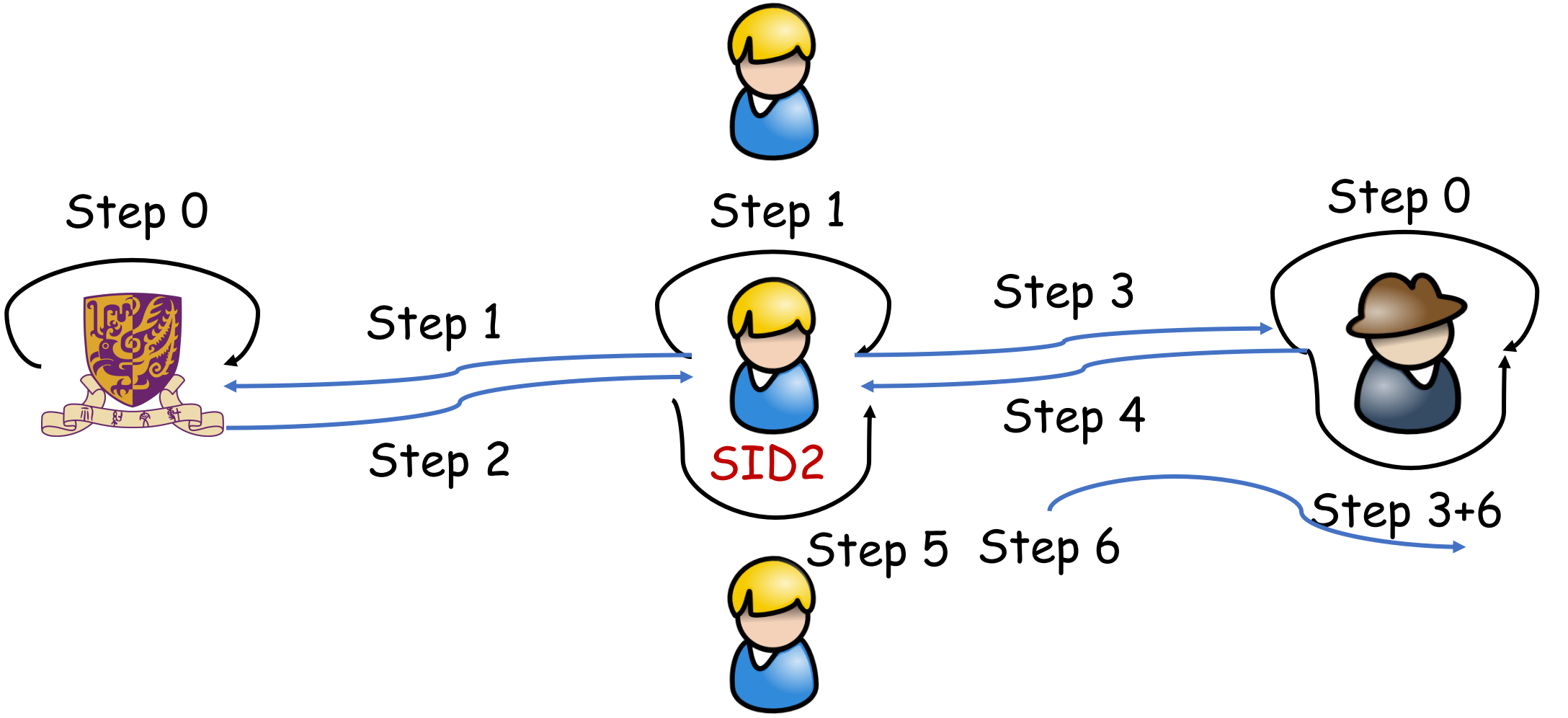
(will re-emphasize it in the future lectures like P6/P7)

Scenario: Students submit reports to Blackboard

- Traditionally, we validate server's identity in TLS and check student's identity via her username/password.
- Here, we validate student's identity via her certificate that is signed by CUHK. For simplicity, we assume that Blackboard can directly access CUHK root certificate, just like modern browsers.



The Overall Workflows



The Detailed Workflows and Marks

	CUHK.py	Student.py	Blackboard.py
Step 0	Generate root cert and key (2’); Listen (1’)		Listen (1’)
Step 1		Input SID/2/3, generate key pair, send CSR request (2’)	
Step 2	Receive the request and Sign it, Send back Cert2, and Student displays “SID2 sign finished” (2’)		
Step 3		Initiate request to B with [SID2, Cert2(~~PubK2~~)] (2’)	Check it using CUHK certificate (2’)
Step 4			Generate session key, Encrypt it, Send (2’)
Step 5		Decrypt session key (1’)	
Step 6		Send 10*msg + MAC (3’)	Verify MAC, output (2’)

Submission Guideline

- Msg: “This is submission from SID1/2/3.\n” Multiply it by ten times.

- **Zip** the following into one zip file and name it “StudentID_lab.zip”
  - **Three Python3 files**: CUHK.py, Student.py, Blackboard.py;
  - **README.txt** to explain some important matters you think;
  - **Claim.pdf** (signed with your signature) to claim your contribution and list all the reference code links (e.g., StackOverFlow and GitHub links) that you use;
  - Note that the quality of your code may affect your scores; (Very) similar code will be **punished** for both students.

- Deadline: ~~18:59 on 30 Nov~~ (more time; extended to **23:59 on 4 Dec 2022**)
- **Late submission will be deduced by 2 marks per day of the delay.**

Further Notes

- You can use any libraries (e.g., pyOpenSSL) and do any Google search, but make sure that you list all the reference code links, including the homepage of all the libraries you have used.

- If you are not familiar with Socket programming, I am fine with that you create a Main.py to invoke (!only invoke) the other three Python files and use files as a communication channel.

- More questions?