INFO2222 Project

1 Security Part Description

Design and implement a secure end to end messaging tool.

Basic exemplary flow:

1. In a page, user A logs in, typing username, pwd
2. If successfully log in, showing friend list, could contain just one; if log in fail, show failure reason.
3. After both A,B log in (in two pages, assuming they are "friends" in the chat), A sends a message (the personalized testing message will be notified before the deadline) to B securely, showing at B's side.

Template. We have provided a website template so that you can run a server and show corresponding sites with the prepared the html pages. While the control functions are located at the corresponding Python files. You can just modify and add function in corresponding Python files. You may want extra package to use advanced libraries.

Examine criteria:

1. Properly store passwords on the server
2. When log in, first check server's certificate (e.g., you can manually create one using a hardcoded CA public key in your code)
3. Securely transmitting a pwd to server (leveraging secure protocols or design the secure transmission properly)
4. Properly check whether password is correct (at least use the simple method that defends against offline pre-computation attacks)
5. Securely transmitting the message from A to B, even the server who can forward communication transcript cannot read the message, or modify the ciphertext (leveraging secure protocols or design the authenticated secure transmission properly)

Reporting requirement.

1. explain in one or two sentence how you address each of above items
2. show screenshot as evidence, if you can demonstrate intermediate executions in extra page, would be even better.
3. clear identify how group members divide the tasks.

Submission deadlines. The milestone report about the security part (and corresponding code) will be due on Saturday mid-night of W8. **Please start early**, there will be another usability part of project, details will be added very soon (about W6), the final report due Saturday mid-night of W10.

Remark. The template and code were just an example, if you prefer to do it in other framework, or using other language, it is OK. Just to make sure you can demonstrate that you properly implement the security features listed above.