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 —— 15 points
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) — 15 points
3. Securely transmitting a pwd to server (leveraging secure protocols or design the secure transmission properly) — 10 points
4. Properly check whether password is correct (at least use the simple method that defends against offline pre-computation attacks) —— 10 points
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) — 40 points
6. Clarify of the report. — 10 points

There are also 20 points bonus if done well or extra functionalities are added, and for adjustment on single-member team.

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.

4. no explicit word requirement

Submission deadlines. The milestone report about the security part (and corresponding code) will be due on Saturday mid-night of W8.

Remark 1 *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.*

2 Usability Part Description

Expand the basic web based E2EE (secure messaging) to be a website of support system for undergraduate School of Computer Science University of Sydney students to share experiences and seek the necessary help (if needed) for their academic studies. It should also have a knowledge repository where students can share reading or learning materials that they found useful to understand challenging computing concepts.

You already have an account and messaging service that allows pair-wise communication among students themselves and to specific academic/administrative staff.

Besides the Login, Register, Messaging (view, send), Regular User role, your website should also have functionalities like following (to be assessed in last activity)

- Data/Info hierarchy – how you organize user generated contents
- Admin Role - delete/mute user, delete a course guide
- One specific user function – depending on your user investigation.

In this part of the project, you are required to design the website with usability and accessibility in mind. A series of recommended activities will be provided in this document as a guide for your team's action plan and discussion. It is advisable that you pace yourself and utilize the practical session to collect feedback on your project from your tutors and peers through the mini-presentation session. Starting from Week 8, you can use the lab to do mini-presentation to collect feedback from both tutors and peers on pieces of work that have been produced. It is not necessary for presentation slides to be used.

Hint: Think about the type of feedback that you would like to get and select the results and work to be presented. you will need to prepare a prototype of the website to conduct a usability test of your website to the tutor and peers in labs. During this presentation session, you will need to demonstrate a typical scenario in which your website will be used by your intended user(s) together with the core requirements.

Submission deadline. The final report about the usability part (and corresponding code) will be due on Weds mid-night of W11.

2.1 Recommended Activities

Step1: User Investigation. During this phase, you are to investigate your chosen group to determine what they need from your website. To make things easier, your group can concern yourself with a single very specific type of user:

- Students – this can range from any students starting just starting their program of studies to final year students. It can also include students transferring into a computing program from other USyd schools.
- Alumni – graduates who are willing to give back to their alma mater and to guide their juniors

- SCS/administrative staff – this can include program managers, academic advisors and administrative staff responsible for the running of program operations that affects students' academic performance.

Perform a PACT analysis for your chosen group. You will likely still find that your selected group is too large and complex but your analysis should help you identify what you know about your target group and what you need to find out during your investigation to narrow your group down to a single persona.

Step 1: Expected output: — 20 points.

- Outline of the user investigation process (surveys/interviews, how many?) that your group has used to narrow down your target user.
- Research materials used to collect data about your target group
- A persona document outlining your target persona
- Based on your findings above, gather content (collection of documents) relevant to the interest of your target persona. This should be in document form before you convert it to your website and must keep it updated with any changes. Ensure you cite all sources and quote where you have copied text verbatim.

Step 2: Navigation design. There will hopefully be a lot of information from Step 1 in many potential categories. As well as this, your website will need to include the following 'user' actions stated in the core requirements in addition to actions specified specially for your own target user group. Conduct a card sorting session with some of your target user group and use your results to create the navigation map (site map) of your website.

Step 2: expected output. — 20 points.

- Outline of card sorting session along with all materials that was used.
- Information architecture of your website

Step 3: Design-Evaluate (Prototype (paper or digital)). Based on the information architecture that you have from the previous phase, brainstorm and create sketches of your website. Create a prototype of the best design and perform guerrilla test with target users using this prototype. Each of your team member should take part in the guerrilla test, at least one participant is outside of your team.

Step3: expected output. — 20 points.

- A prioritized list of additional features?
- Outline steps taken to determine the 'best' design to be prototyped
- Paper or digital prototype,
- Mini-report that outline of how guerrilla test is conducted, actual raw results, materials used and findings of the test.

Step 4: Design-Evaluate (Hi-Fi Prototype). Focus on converting your (improved) prototype (paper or digital) to the real web server. Do this incrementally and perform evaluations (e.g., think aloud test) to ensure that you are on the right track.

Step 4: expected output: — 20 points.

- Incremental development plan (two iterations at least)
- Outline of evaluations conducted

- Demonstrations of the functionalities mentioned at the beginning, admin roles, the user specific function etc.

Remark 2 *Your output in Step4 does not need to be perfect, we care more and the markings will focus on your improvements over each iteration.*

Step5:Final report. — 20 points.

- It is a collection of all the previous outputs in a neat format. The template is given.

Bonus step.— 20 points. You can re-use and extend many of your existing implementations on the security project to have public and private mode of posts. The default mode of posts could be public. The private mode will be visible to only specific role or user (i.e., you have to use encryption properly).