Course Name: Secure Software Engineering

Course Code: COMP SCI 7412 & 7612

Assessment Component: Software Design and Prototyping Project (40%) – Group and Individual Assessment

Project Description

Topic: A Privacy-by-Design Home Services Application during COVID-19

Image that COVID-19 is still around.

COVID-19 is a global pandemic affecting over 200 countries, after its first recorded outbreak in December 2019. To counter its spread, numerous measures have been under-taken by public health authorities, e.g., quarantining of people, lock-downs, curfews, physical distancing, and mandatory use of face masks. Identifying those who have been in close contact with infected individuals, followed by self-isolation (so called contact tracing) has proven particularly effective. Consequently, contact tracing has emerged as a key tool to mitigate the spread. However, manual contact tracing, using an army of "detectives" is not trivial and has proven challenging for many countries. Notably, it is difficult due to the rapid and exponential growth patterns of the virus and the increased demands on qualified human resources. Thus, in many countries it has become extremely difficult to perform manual contact tracing.

Government authorities around the world, together with industry, have sought to address the challenge by developing contact tracing applications and services. A plethora of apps and services are still being deployed around the globe. Proponents argue that the low cost and scalable nature of contact tracing apps make them an attractive option for health authorities. Despite this, contact tracing apps are not universally popular, with a number of prominent critics. They have proven particularly controversial due to potential violations of privacy, and security consequences from the mass-scale installation of (rapidly developed) apps across entire populations. Despite attempts to alleviate these concerns by both governments and industry, it is well known that the anonymization of individual information is a challenging problem.

Meanwhile, people's activity, including cross border travel, has been restricted during the pandemic. For example, in South Australia, there are level systems define the activity restrictions (requirements related to density, mask wearing, private activity cap, sports, stay at home, etc) and travel restrictions (restrictions related to COVID-19 test, entry to SA, quarantine, etc). Considering that it has been more than two years into the coronavirus pandemic, nations has accepted that Covid- 19 is not going away, despite high vaccination rates drastically cutting the number of hospitalizations and deaths. Although we can protect ourselves by staying at home, it's not the best way to "live with covid". Therefore, how to help people meet each other / date under restrictions could be a new challenge to software industry.

In this project, you are required to (i) investigate into the current status of COVID contact tracing and Home Services apps; (ii) research and understanding the potential privacy issues in kinds of contact tracing and Home Services apps from different regions/countries; and (iii) design and implement a **privacy-by-design** solution to protect user privacy as much as possible while ensure the essential performance, e.g., the accuracy and effectiveness of contact tracing, the restriction information notification, the basic functionalities for a Home Services app.

Some Useful Links/References

J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy,"Bluetrace: A privacy-preserving protocol for community-driven contact tracing across borders," Government Technology Agency Singapore, Tech. Rep, 2020

"COVIDSafe," https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

"COVID SAfe check-in", https://www.covid-19.sa.gov.au/restrictions-and-responsibilities/covid-safe-check-in

C. Troncoso, M. Payer, J.-P. Hubaux, M. Salath´e, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioliet al., "Decentralized privacy-preserving proximity tracing," arXiv preprint arXiv:2005.12273,2020.

"Analysis of DP3T between scylla and charybdis," https://eprint.iacr.org/2020/399.pdf

L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-D orner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying SARS-CoV-2 transmission suggests epidemiccontrol with digital contact tracing," Science, 2020

"In Coronavirus fight, China gives citizens a color code, with red flags," https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

"How to create a mobile travel app?" https://theappsolutions.com/blog/development/build-mobile-travel-app/

Implementation

Programming languages are open to implement your system. Your system should be designed for public distribution. All milestones should be accompanied by a README.txt file containing installation instructions and, as necessary, installation scripts. If users cannot run your system, they cannot use it. If we cannot run your system, we cannot grade it. When building a system in industry, it is generally a good idea to extend existing components rather than build your own. For example, there are many third-party systems and tools available for building web services. Some can prevent buffer overflows and other vulnerabilities. But if you believe it makes sense to incorporate other third-party code into your project, you must clearly acknowledge the source of that code in your documents and demos.

Milestones

This project is broken down into three phases. For the Final milestone, you will submit an individual task report and a group task report of the project (up through that milestone). The high-level description is provided below:

	Individual tasks and due dates	**Group tasks and due dates**
Milestone 1	Individual task 1 – Requirement Elicitation, Security/Privacy Goals, and Functionality Documentation	Group task 1 – Design Sketch and Decisions

Milestone 2	Individual task 2 – Detailed Design and Modelling	Group task 2 – Product Design and Preliminary Implementation
Final **40 marks**	Individual task 3 – Final Individual Report (12 marks)	Final presentation + demonstration video (14 marks) Group task 3 – Group Project Report (14 marks)

Note: There is no submission required for Milestone 1 & 2, so that you can use the description and requirements in Milestone 1 & 2 as checklists and ensure that your project is progressing smoothly. Please include the reports of Milestone 1 & 2 in your final Group Project Report.

The list of individual tasks:

I1. Requirement Elicitation and Security Goals/Functionality Documentation – You are asked to elicit and document 5 new security/privacy requirements (i.e., features) for the chosen project. You are expected to carry out some research on the different aspects of the project for eliciting five new requirements (i.e., features). The elicited 5 new security requirements need to be documented using the template below (i.e., ID, name, description, and rationale/security goals).

ID	Name	Description	Rationale/Security Goals
R01	Renovating a bathroom via the app	A member whose identity has been verified may have the option to start working on renovating a bathroom of a client. A member may also meet the client in person to discuss the plans or cancel a job if they feel unsafe.	For a job, getting everything that was mentioned in the job description is one of the most important features that clients are going to rate members for.

Rubrics:

1. The requirements should be related to the requirements for the project in Secure Software Engineering.
2. The requirements should be unambiguous and complete.
3. The requirements should properly balance between security/privacy goals and functionality.

I2. Detailed Design and Modelling – You are asked to perform detailed design and modelling of the 2 requirements of your individual Task 1. The design and modelling output must include a detailed class diagram for the two requirements used for analysis and 2 sequence diagrams for the chosen requirements. You are expected to use a suitable modelling tool (e.g., LucidChart, MS Visio, or OmniGraffle). The detailed design and modelling task of the project must be formalized into a document suitable for a development team to implement.

Rubrics:

1. The sequence diagram must include actors and at least 3-4 objects and timeline of the objects. A short description must be included to describe each of the sequence diagrams.
2. The class diagram is detailed and captures all aspects of the two requirements modelled. A short description must be included to describe key aspects of the class diagram.
3. The class diagram includes correct relationships (e.g., aggregation, composition, etc.) and classes include 2-3 relevant attributes and 2-3 suitable operations.

I3. Final Individual Report – You are expected to report what you have contributed to the final project. The report should introduce the security or privacy issue you focused on and give a description of the related requirement, feature design, and solution you implemented. Please demonstrate the methodology and the functionality of the implementation.

Please also include your reflection of the project. For example, what you have learned in this project (e.g., programming skill, project management, or team work) and what could be improved in the future.

The list of group tasks:

G1. Design Sketch and Decisions – Your team is asked to work in your assigned group to brainstorm high level design options and perform design sketching based on the requirements and **security/privacy goals** from the individual Task 1 (use requirements from group members). Then draw a storyboard that should illustrate the usage scenario and interaction between actors and the system (see an example below). The storyboard must have at least 5 sketches. Sketches can be done on paper, electronically or whiteboard. The group work can be captured as a photo which can be presented in milestone. Based on the brainstorming process from the sketches and storyboard, a team is required to document at least 5 design decisions and their rationale using the suggested template.

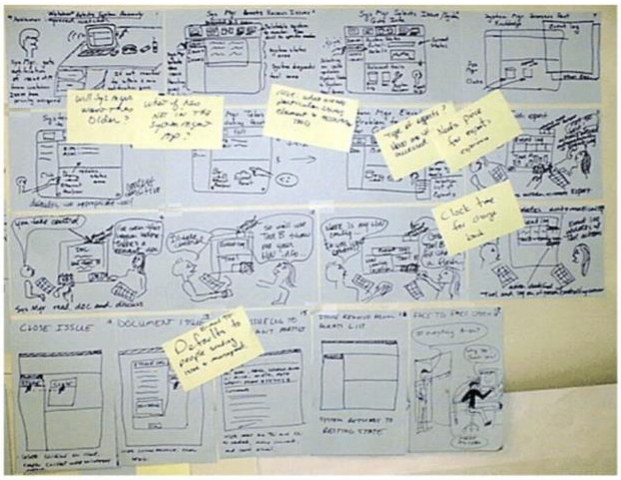

Figure 1. An example storyboard of a software system.

Table 1: The template of the design decision.

Design Issue	(*What is the design issue*) The software system has no authentication/authorization mechanism
Context	(*Why the issue needs to be addressed*) The system hosts sensitive data, which should not be made accessible to every user.
Quality Attributes	(*Which quality attributes will be affected by the issue*) Security, Performance, Availability
Solution	(How to address the issue) Incorporate authentication/authorization mechanism
Description	(*Brief description of the proposed solution*) The system should incorporate a two-layer access mechanism – authentication using Brokered authentication pattern and authorization using Role-based authorization pattern.
Rationale	(*Why this solution is selected*) The authentication mechanism will ensure that the user is already a registered and legitimate user of the system. Furthermore, the authorization mechanism will ensure that the user will not access any data or service for which the user does not have access privileges.

Rubrics:

1. The sketches are sufficiently detailed, suitably labelled, and easily understandable.
2. The design decisions are suitable for addressing the selected design issues to be addressed. At least one design decision incorporates one design pattern.
3. The design decisions and their rationale are appropriately documented using the provided template.

G2. Product Design and Preliminary Implementation – Your team is asked to design systems that are privacy-by-design based on the requirements you have selected to work with. Each group will be using this design when implementing a prototype as requested in other tasks.

Rubrics:

1. Designs are reasonably and correctly designed.
2. Designs should be consistent across different features (i.e., requirements).
3. Designs should be appropriate and natural for your system's functionality and expected scale.

G3. Project Presentation, Report and Demonstration Recording

The slides presentation should include no more than 12 slides excluding the title and the conclusion/reference slides. The presentation should highlight the security/privacy requirements addressed, the system overview, the class diagram, the key design decisions, the user interfaces, and the developed prototype. Each member of the team must actively participate in the presentation.

Your team will summarize your completed course project in a report (at most 10 A4 pages, excluding references and appendix), and demonstrate the final deliverable by video recording (prototype explanation and demonstration). Your team will be required to submit a final demonstration of your prototype as a video (i.e., a YouTube URL) and a zip file of the source code.

Rubrics:

1. The slides are of good quality/professional and include all the necessary information.
2. The presentation engages the audience and is completed on time.
3. The prototype must be executable.
4. The prototype must include at least 5 requirements.
5. The video recording must be professionally edited with a high resolution (at least 480p) and included some explanation.