**SYSC 4907 Project General Structure**

**Based on the meeting discussion of 09/16/2021**

The main purpose of this project is to develop a platform that can be used by other developers to:

1. Store and manage the significant amounts of evidence
2. Ensure traceability to evaluation criteria

The general structure of the project could be split into two main sections:

* Front-end (UI)
* Back end
  + calculation and logic
  + database for evidence

**Front-end:**

Front-end may have some of the following features:

* User Login
  + Could involve using:
    - Access control Matrix [ABAC/RBAC]
    - Password Mechanism [SHA-256]
* Upload/Review Evidence
  + Could involve using:
    - File Management Mechanism [read only/write only]
* Search for Evidence by tags/date
* Build relationship between evidence, code/program, and security criteria like CC (tag/classification/…)
* Maybe consider compatibility of different security evaluation criteria (expansibility)
* …

Front-end format could be chosen between the following option, the reason for the selection could reflect in the report:

* Webpage [HTML]
  + Easy to write and modify [Sustainable development]
  + Lightweight; Could be used anywhere
* Desktop Graphical User Interface [Java GUI]
  + Better display on size and pixel
* Some refs related to Web vs GUI:
  + <https://www.nngroup.com/articles/the-difference-between-web-design-and-gui-design/>
  + <https://stackoverflow.com/questions/648305/when-to-choose-between-web-interface-and-native-gui>
  + <https://www.boddunan.com/articles/education/19-engineering/7550-gui-versus-web-page-design.html>

Need come up with program use flow after reading the documentation Prof provided.

* Steps
  + …

**Back End:**

Calculation and logic should enable to process the following commands from the front-end,

* Login
* Update/Review
* Search
* …

Database for evidence should enable to store evidence:

* The format of the evidence needs to be future discussed,
  + Quote from “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model”, pp. 11,

The CC addresses protection of assets from unauthorized disclosure,

modification, or loss of use. The categories of protection relating to these

three types of failure of security are commonly called **confidentiality**,

**integrity**, and **availability**, respectively.

* + The type of tags could be considered from the following three points:
    - Confidentiality
    - Integrity
    - Availability
  + Can also be classified following the specific criteria classification (if we need to use criteria as tag), like:
    - Common Criteria
      * Security Functional Components
      * Security Assurance Components
* The storage could include but not limit to tags, date, update location and user information
* The detailed way of storage varies based on evidence type, will be future discussed.

**Development related:**

Version Management tool for this project: GitHub

Programming languages: To be determined

The questions left after the meeting:

* Is Python a selectable programming language in this project?
* What format will the evidence be? **[Need investigations before asking]**
* …