A Platform for Managing Security Evaluations

Project Proposal
SYSC 4907 Fall 2021

Team Members
(Last name in alphabetical order)
Zijun Hu 101037102
Tiantian Lin 101095243
Jiawei Ma 101034173
Ruixuan Ni 101092506

Supervisor
Jason Jaskolka, Ph.D., P.Eng.

Date: October 22nd, 2021

Table of Contents

1. Introduction

1.1 Project Introduction

Nowadays, the reliance on information technology from people is increasing. Corporations are paying more attention to protecting their systems and products with well-implemented security mechanisms in this environment. There are already multiple security evaluation criteria for computer security certification (for example, the Common Criteria [1]). These criteria provide standards for systems to be checked to ensure if the security features in the TOE (target of evaluation) work correctly in these systems.

The evaluation results would help customers to determine whether the products satisfy their security requirements. That is one of the reasons why corporations need to provide evidence to prove that they have met the standards in criteria. These pieces of evidence may come from many different sources, especially for large and complex systems. A platform that can store and manage the evidence could help evaluate and check the security of the system.

This project aims to design such a platform that would allow developers to upload security evidence. This platform can store and manage a large amount of security evidence, and it can also provide evidence tracing functions for subsequent security assessments.

1.2 Platform Development Requirements

The platform will store evidence that provided by developers. For now, the platform would only consider the evidence in text format. Thus, the platform should allow developers to upload, access, and manage evidence. Besides, authorized developers will be able to search the security text evidence by typing some keywords to help them find related evidence easily.

To ensure the security of stored text files, all existing evidence should only be accessed by authorized developers. Therefore, the platform should use the developer's username and password as identity verification to identify the developer's authority. The unauthorized user will not be able to access and upload any text evidence.

To increase the performance and usability of the platform, authorized developers can use this platform to manage text evidence anytime and anywhere. To reach this goal, we designed the platform to interact with developers through a web page. Developers can access the platform using any commonly used web browser such as Chrome, Safari, Firefox, Microsoft Edge, etc.

Besides, there may be various accidents that cause the stored text evidence to be lost. To avoid this type of issue, the platform should be able to back up the different versions of text files based on the edited time. Therefore, the authorized developer could recover that text evidence once any evidence is lost or deleted by accident.

1.3 Progress Measurement

There are four milestones set for this project. They are *Design*, *Development*, *Integration* and *Documentation*. The details related to each milestone will be discussed below.

First Milestone: Design:
During this milestone, the main objective is to design the project/program, including timeline setup, development tools and models selection, UML diagrams and strategies design.

There are four members in the group. It is essential to make sure everyone's thoughts and efforts are consistently directed toward the above goal. A project with a good design as the beginning could help to prevent various risks such as missing requirements and redundant programming. And through a good design, we can always make sure each team member is on the same page.

This milestone has several procedures: making a plan for the whole project, analyzing the project's functional and non-functional requirements, creating several UML diagrams, choosing an appropriate model and pattern to develop the program, and unifying the programming development environment and tools.

By the end of milestone1, our group should submit a qualified project proposal. The proposal should illustrate a clear view of the project and the basic plan for the project. Besides, the team will choose the most suitable design model and pattern by weighing the benefits and disadvantages of each model and strategy. Last but not least, it's better to have UML notations such as class diagrams, sequence diagrams, and object diagrams to present the project's requirements and components. Those diagrams will help us while developing the program.

Second Milestone: Development of the Program Separately:
In the process toward milestone2, our group would start developing the program. The project will build on the Client-Server pattern. Using the design pattern, the program will be split into several parts. It will ensure that each member contributes equally and achieves the program's high cohesion and low coupling.

By the end of milestone2, all functional and non-functional requirements will be implemented entirely. Although there may still have some bugs in the program, the main objective of Milestone 2 is to ensure that each component in the program can execute and run as expected by the requirements without compiling errors. Furthermore, the program should be prepared to integrate and be prepared for the quality assurance testing.

Third Milestone: Integration of Different Parts, Test and Fix Bugs:
After each member completes their development, there must be a lot of faults in the program during the integration. Therefore, we need to integrate different parts, test the faults, and fix bugs to ensure the program will run without any unexpected states or behaviors such as the whole platform crashes.

In milestone 3, the entire program will be integrated into a whole through the developed interfaces. We would create different test suites to ensure that there would be no unexpected states, the whole program should run as expected, and the tests would cover all codes.

By the end of milestone 3, the development of the entire program should be finished. The program should run as expected. And the program should not have any errors that can cause the failures and be observed by users.

Fourth Milestone: Documentation and Presentation:
After completing the platform, the next goal will be creating documents that will help users get familiar with the platform.

To reach the objective, the team will create documentations and give presentations related to the work done. It will help users understand the program in three dimensions: what it is, how to use it, and why to choose it.

By the end of milestone 4, all documentation, such as the final report and the oral presentation, should be completed and delivered. And all unfinished work in the previous milestones should be completed.

2. Background

Security testing and vulnerabilities management tools are already widely used in the system development life cycle. Tenable is one of the vulnerability management tools [2]. It can be used to manage risks and monitor the changes in attack surfaces. It could also analyze threats, vulnerabilities, and asset data to evaluate the significance. These tools usually concentrate more on risk assessment, which means they tend to detect the potential threats and vulnerabilities of software for developers and help them establish protected strategies.

However, these tools do not pay much attention to the management of evidence which used to prove that the system or products satisfied the evaluation criteria or requirements. It makes it difficult for security evaluators, regulatory authorities, and developers to trace the evidence or related evaluation criteria and standards.

3. Project Description

3.1 Purpose

This project aims to develop a platform that developers can use to store and manage the security evidence generated during the entire system development lifecycle for future security assessments. When developers design large and complex systems, the storage and traceability of security evidence become a significant problem. The reason is that when designing and developing large-scale systems, the sources of evidence are complex and huge. It makes the follow-up security assessment difficult. Therefore, this management system can help security analysts collect security evaluation data and help developers manage evidence.

3.2 Structure of Project

The pattern of the project is based on the Client-Server pattern. The structure of the project is divided into two main sections: Front-end and Back-end. The primary purpose of the front-end is to interact with the user, allowing users to upload/view the evidence and display needed information. The back-end includes a server and a database to categorize and store all involved evidence and information.

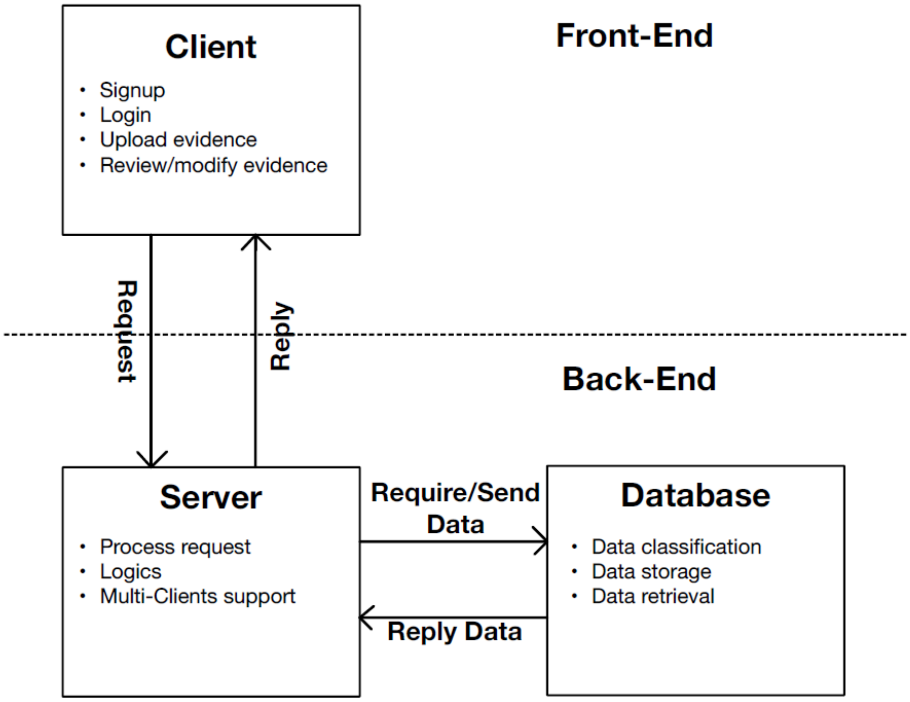

Figure 1 Project Structure

3.2.1 Front End

In this project, the front-end will be designed and delivered in webpage format. The page will be written in HTML and styled using CSS. Users need to either sign up or log in using their username and password via the login page to use the system. A security password mechanism will be used to safeguard the system. When users sign up, the system will enroll them into the access control matrix depending on their role to ensure that they can only read/write to subjects their privilege allows. After users log in, they can choose to upload new evidence or review existing evidence.

To upload new evidence, users need to provide related information via the evidence upload page. The page will provide an online form for users to fill. Required information includes but is not limited to the type of evidence, related project change information and comments to the evidence. The purpose of doing that is to help categorize the evidence later and ensure the traceability of the evidence history.

As well as the upload page, there will be a search and review page provided to users for them to search and review the existing evidence. The system will offer several filters to users to explore the evidence they want. The evidence can be filtered by tags, evidence type, upload users or last modified time.

3.2.2 Back-end

The Back-end section will be split into two sections: Server and Database. The server's primary purpose is to interact with the front-end and provide service for users. The database aims to store data and provide data to the server when required.

3.2.2.1 Server

The server will include logics that can process the request received from the front-end. It will provide services including new user registration, login, upload or review evidence, evidence information management, etc.

When receiving new evidence from the front-end users, the server will process all related information, including but not limited to tags, modify/creation date, username, related project, etc. Then it will save the data to the database by using the database interface. As well as saving data, when the server receives the search/review requests from the front-end, it will also request needed information from the database using the interface.

Moreover, the server will achieve multiple clients supports. The server will process each front-end request in a separate thread so it can provide service to multiple users simultaneously.

3.2.2.2 Database

The database will store the user's account information and the text file information uploaded by users. The user's account information includes the user's login name, encrypted password, login history and so on. The information of the text file uploaded by the user includes the upload date of the file, the user who uploaded the file, the tag of the file, etc. The database will be written in SQL to achieve database creation, data storage, data retrieval, and data classification.

The server can request data from the database based on user requirements. According to the request from the server, the database will search for the data that meets the conditions in the database and returns it to the server.

4. Methodology

4.1 Program language selection——Python

In this project, we would need to implement an application based on the Client-Server (CS) pattern. Our group decided to use Python as the development language. Python is a high-level scripting language in programming with an extensive library. It has modules and packages which support functions like data management or network transmission [3]. Python also supports accessing databases like MySQL with wrapper, which simplifies data storage and transmission functions [4]. These functions could help our group to build web pages as interfaces, establish databases to store evidence and combine these different modules together.

We have also considered Java. Compared to Java, Python is a more readable programming language and easier to learn. Python is also more efficient than Java in development. Besides, all of our team members have essential experience in Python programming. Our group believes that Python is a programming language that is more suitable for our present project architecture and development plan.

4.2 Software design pattern——Client Server

The Client-Server design pattern is a network architecture consisting of a server and several clients. It allows the server to provide service to multiple client components. In this pattern, users could interact with the client, which is the webpage in our project. The client would pass these requests from users to the server. The server would be responsible for processing these requests and passing the result.

Our group has decided that we are going to build a platform with web pages as the user interface and databases to store evidence uploaded by users. This primary structure suits the Client-Server framework. Client-Server is also a design pattern widely used in web application development.

4.3 Web Interface vs Graphical User Interface

Graphical User Interface (GUI) is one form of user interface (UI) that allows users to interact with the program to perform needed commands [5]. Using GUI, the designer could easily control each pixel on the users' screen and the access direction. As well as that, the GUI can efficiently guide the user to view the information/pages the designer wants. Also, it can force the user to enter information before entering the next step by using the pop-up windows [6]. However, it makes users' operation flexibility become lower. At the same time, it also takes longer for users to familiarize the system and operating methods.

Web Interface is a kind of interface that requires the users to access via the web browser on their phone, computer, or tablet. Compared with traditional UI, it provides users more flexibility and is accessible to update. Users can access through any smart device with a browser. At the same time, because the webpage itself is stored on the service provider's server, developers got chances to update the web page easily without asking users to download any updates packages.

After balancing the pros and cons, the webpage format was selected for the front-end development in the project due to the ease of application updating and the flexibility on accessing.

5. Timetable

According to the Project Guideline, our team decided to set the project completion time. Besides the deadlines in the Project Guideline, we would also set and add the deadline of the four milestones to the timetable to make our plan more feasible. All details about the milestones are mentioned in section **1.3 Progress Measurement**.

To prevent potential risks that may delay our process, such as illness, our group plans to complete each task and milestone three to five days before the scheduled deadline. If we complete each task or milestone ahead of our schedule, we can double-check our program for existing problems through the remaining three to five days.

Task Name	**Schedule Complete Time**	**Deadline on Guideline**
Project Proposal Draft	October 1st, 2021	October 1st, 2021
Milestone1 Completion	October 20th, 2021	N/A
Project Proposal	October 20th, 2021	Noon of October 22nd, 2021
Progress Report	December 5th, 2021	December 10th, 2021
Milestone2 Completion	December 31st, 2021	N/A
Oral Presentation Preparation	January 22nd, 2022	January 24th, 2022

Milestone3 Completion	February 10th, 2022	N/A
Draft of Final Report	February 23rd, 2022	February 28th, 2022
Poster Fair	March 14th, 2022	March 18th, 2022
Milestone4 Completion	April 8th,2022	N/A
Final Project Report	April 8th, 2022	April 12th, 2022

6. Potential Risks and Mitigation Strategies

Potential Risks	Instance	Mitigation/Solving Strategies
No time to complete any particular progress before the planned deadline	A requirement could not be fulfilled before the designed deadlines due to other exams, quizzes, and assignments.	-Plan to finish the work ahead of the designed date as much as possible. Allow enough time for various accidents. -If multiple requirements are not fulfilled, choose the most important one and work on it first.
Any member gets an illness during the development.	Any member caught a cold. And he/she cannot participate in group work within a week.	-If we have enough spare time, the other group member could finish their part first. Then, we can help the sick team member complete their task before they recover. -If time is rushing, we need to make tradeoffs to verify whose part is more important. If the sick group member's part is more important, then any other member needs work on the ill member's part.
Structure or strategy change in the middle stage of progress	Select Client-Server pattern and start programming. But halfway through, we found that the Client-Server pattern could not provide what we wanted and decided to change to another mode.	It depends on how much we did. -If we just start programming, we could switch to another design pattern and re-program what we got. -If we programmed a lot, we need to stick to the original structure. Try to solve the problem or find the solution.
Meet problems when coding, which makes progress behind schedule	When programming, a member found the problem of sending and receiving sockets in TCP/IP. There are many bugs, and the member is not familiar with the API. And the problem delayed the design date by ten days.	-Plan and provide a feasible timeline. -Try to find another way to replace the algorithm.

7. Discussion

7.1 Individuals

7.1.1 Zijun Hu

As a computer system engineering student, I have learned system security, software communication, and development knowledge. I will focus on the front-end development and the program logic between the front and back-end interaction in the project development process. I will use the knowledge I learned in the Introduction to Software Engineering course to make the development process more efficient and systematic. As well as that, I am currently taking an elective course called Fundamentals of Web Development, which will also help me when developing the front-end section for the project.

Since my team members are all coming from the Software Engineering program, I might be less professional than them in software development. But at the same time, I have some knowledge that they do not possess, especially on computer networking and communications software. This knowledge will help me fill the vacancies in the team and make the interaction between the front and back ends of the project more comprehensive.

7.1.2 Tiantian Lin

As a student of software engineering, the design of this project can be connected with many aspects of what I have learned from the previous three years. So far, I have taken many courses related to software, such as database management, software design and software requirements engineering. In this project, I can use what I have learned in these courses to design and develop a back-end system. In the early stage of the project, the knowledge of software architecture can be used to design the back-end system's different components and frameworks. I could design the UML diagrams, sequence diagrams and state diagrams before developing the entire system. In addition, through the internship, I also have some experience in automated test development. Combined with the software verification course currently being studied, it will also help the test development process for the project.

7.1.3 Jiawei Ma

Since my four-year studies in Software Engineering, I have learned and practiced a lot related to programming and software development. My most significant strength in programming skill is Java programming on both front-end and back-end. Similarly, I am also good at other programming languages such as C++ and C on the back-end. Through the project and program design courses, I also have dramatic knowledge of project requirement design and requirement analysis. Therefore, I would apply my project and programming design knowledge, programming skills, and communication skills to this project with my group members.

Besides, through the Co-op study as quality assurance, I now can test the program manually and automatically after each development phase. Despite not being good at Python and web programming, I will still communicate and cooperate with my group members by studying related knowledge and applying it to the project.

7.1.4 Ruixuan Ni

I am a student studying in the program of Software Engineering. Since this project requires a complete software development process, this project is directly related to what I learned during my undergraduate study. In the early stages of the project development, I could contribute to the development of requirements, design of architecture and details (for example, drawing UML diagrams). For this project, our group plans to develop a web platform to manage evidence of security evaluation. In the implementation phase, we might use Python, Django and MySQL. I have learned the fundamentals of Python in school and have practiced Python projects during co-op. I have also learned basic SQL commands. This means I could also contribute to the project implementation in the front-end, back-end and database. Generally, since most of my group members are in the program of Software Engineering, we would prefer to cooperate in all stages of development.

7.2 Group

Our team members are from software engineering and computer systems engineering. Everyone has studied or is studying the SYSC4810, *The Introduction of Network and Software Security*. Therefore, for this project, the safety evaluation management platform, the team members can use the knowledge they have learned to have a general framework. Besides, all team members have studied SYSC3120/ SYSC3020. All members can contribute knowledge about analyzing requirements and designing the project to satisfy the requirements. In addition, each team member has their field of expertise, including but not limited to web design, database management, automated testing development, network transmission protocol, software architecture design. These skills are all essential for the realization of this project.

8. Components and Facilities

There is no specific item that needs to be acquired/purchased.

9. Conclusion

In conclusion, the four milestones and the timetable will help allocate development tasks reasonably and achieve continuous and effective development. As well as that, the discussion on potential risks and mitigation strategies will also play an essential role in avoiding the clutter brought from incidents or risks.

For the project itself, the Managing Security Evaluations Platform will allow users to upload and manage evidence via the web page during the system development process. It provides a tool not only for developers but also for security evaluators and regulatory authorities to evaluate and review the system's level of security. It will help developers store and collect evidence and ensure traceability to security evaluation criteria used in the security evaluation process.

References

[1] "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model," April 2017. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf. [Accessed 27 September 2021].

[2] "Vulnerability Management," Tenable, [Online]. Available: https://www.tenable.com/solutions/vulnerability-management. [Accessed 11 October 2021].

[3] P. S. Foundation, "The Python Standard Library," Python Software Foundation, 01 October 2021. [Online]. Available: https://docs.python.org/3/library/. [Accessed 01 October 2021].

[4] A. Lukaszewski and A. Reynolds, MySQL for Python, Packt Publishing Ltd, 2010.

[5] F. Churchville, "What Is a User Interface?," TechTarget, September 2021. [Online]. Available: https://searchapparchitecture.techtarget.com/definition/user-interface-UI. [Accessed 21 October 2021].

[6] J. Nielsen, "The Difference Between Web Design and GUI Design," Nielsen Norman Group, 30 April 1997. [Online]. Available: https://www.nngroup.com/articles/the-difference-between-web-design-and-gui-design/. [Accessed 1 October 2021].