CS4454 –Secure Software Development Spring 2024

Healthcare System (HCS)

Project Problem Description

You have been requested to develop a healthcare system with the following characteristics:

The CEO of a hospital plans to build a secure healthcare system, which manages patient information securely. A hospital has a CEO, doctors, nurses and staff. A patient can make an appointment, change, or cancel the appointment through the healthcare system directly or by calling a staff in the hospital. On-line appointments are required for a patient to have an account in the system. A patient or staff checks a doctor's available time, with whom the patient makes an appointment. The appointment is recorded in the system, and updated whenever the patient change or cancel the appointment. An appointment will be cleared when a patient visits the doctor in the hospital. In case of missing appointments, the system clears the appointments automatically at 8 pm on a daily basis. The hospital does not accept walk-in patients.

When a new patient arrives at the hospital, a staff enters to the system the patient information, which includes patient name, address, phone number, email, social security number, and insurance name. Then the staff creates a patient record for the day visit, and adds the record to a list of patients being served by each doctor. For a returning patient, the staff just finds the patient record and adds it to the list of patients for a doctor. The nurse measures a patient's weight, height, blood pressure, and pulse every time a patient visits a doctor, updating the patient record with the measurements. The nurse also adds the reason of patient's visit to the doctor to the patient record. A doctor can look at the next patient record before he/she meets a patient. After treating a patient, a doctor updates a patient record with his treatment content and, if any, prescription.

A patient can access his/her medical record on-line via the healthcare system, which includes a doctor visit summary, lab result, radiology report, pathology report, allergy information, and prescribed medicines. A patient is required to log in his/her account with ID and password in order to access his/her medical record. If a patient does not have his/her account, he/she should sign in a new account. A patient can see his/her medical record, but he/she cannot change the medical record.

A patient pays for the copay of a doctor visit to the staff just after getting a treatment. A patient can pay it by credit/debit/check/cash. In cases of credit or debit card payment, the card is validated by the card company, and the amount is charged to the patient card account in the card company. Then the card company sends a reference number to the hospital, which is stored with the patient payment information. A patient receives a receipt for the payment.

In addition, a patient pays an invoice (except for the copay for a doctor's visit) for his/her medical services on-line via the healthcare system. The hospital sends to a patient his/her invoice for any medical services using emails. The patient can access his/her account with his/her ID/password to pay the invoice using a credit or debit card. Also a patient can pay the invoice with the invoice number without logging in his/her account. The system generates a receipt for the patient's on-line payment and emails it to the patient if the patient wants to receive the receipt using his/her email.

The system generates a daily summary report at 9 pm every business day and a monthly report at the end of each month. The report shows the information on doctors' performance for a day or a month. The report

contains each doctor name, the number of patients served by a doctor in a day, and health service income. The monthly report is a summary of daily reports for a month. The daily and monthly reports are stored in the system so that the CEO looks at them any time.

Doctors, nurses, staff and CEO are allowed to access their patient records, and payment information on the basis of their permission. A doctor has all permission on read/write on his patient record. A nurse has read/write permission on patient record, but she cannot write treatment. A doctor or nurse can access only his/her patients' records. A staff can create, read and write patient information on a record, and access patient payment information. CEO can read patients' records and payment information, but he cannot write on it. The CEO can look at the daily and monthly reports, and change a doctor and his/her nurse' salaries according to their monthly performance.

Course Project Score table

Course project is 50% of the total Grade. Each group must submit total 4 deliverables for the project.

Course Project	**50%**
--Requirement Specification	15%
--Requirement Analysis	15%
--Architectural Design	10%
--Implementation/Testing	10%

Individual Performance:

Team must keep track of the performance of teammates. Based on number of assigned task and completed task, individual score may be different from another.

Each team needs to send weekly progression report that shows list of tasks assigned to each teammate and tasks completed (must show who completed the task). If your team has not progressed for a week, it is ok. However, you still need to send a report that shows list of tasks assigned to each teammate and tasks completed. Remember, everyone must agree with the progression report before submission. After each phase submission, each team leader must see me for a short meeting regarding team performance.

You are required to develop:

Requirements Specifications (Due date will be announced in the class)

- Develop the use case model for the healthcare system in terms of actors and use cases. Draw the use case diagram and describe each use case using the use case documentation template in the lecture note.
- Draw misuse cases for use cases in the use case model. Point out where a misuse case is added to a use case description. Describe each misuse case with the misuse case documentation template in the lecture.
- Develop the secure use case model along with the use cases and security use cases against the misuse cases. Point out where each security use case is added to the use case description. Describe each security use case with a security use case template.

Requirements Analysis (Due date will be announced in the class)

- Develop the static model for the healthcare system, which depicts the classes and their relationships. A class can be classified as a boundary class, entity class, control class, or application logic class. Define the attributes of each entity class.
- Develop the communication model depicting objects participating in each use case and the sequence of interactions among the objects. A use case is modeled using a communication diagram.
- Develop the threat/object/security service diagram using the class model
- Analyze the threat/object/security service diagram to find the new threats for requirements analysis phase. For each new threat, provide a security measure (security service). Describe new threats and their security measures.
- Develop the security classes on the static model and describe each security classes.
- Develop the secure communication model that depicts the application objects and security objects participating in each use case. Describe the sequence of interactions among the objects.

Architectural Design (Due date will be announced in the class)

- Design the software architectural model for the healthcare system where the model is defined in terms of subsystems and their interactions. Each subsystem should be represented with objects supporting the subsystem. Define the communication styles between subsystems.
- Design the secure software architecture for the healthcare system where the architecture is structured with application and security subsystems, and their interactions. Define the communication styles between application subsystems and security subsystems.
- Analyze the secure software architecture to identify new threats to the software architecture. For each new threat, provide a security measure and describe.
- Revise your secure software architecture with security measures identified above. Describe your secure software architecture.

Implementation / Testing : Due date: (Due date will be announced in the class)

- Develop a running prototype. You need to implement classes using object-oriented language such as C++, C#, or Java, and then integrate them to each subsystem, which should be further integrated into a system. GUI is **NOT** required.
    - **This is not 100% implementation. Teams will implement only selected functionalities.**
- Design test cases that have test data and expected results. Test the prototype using test data to each use case and then record the test results. You are required to turn in your test results with test cases.

Make your assumptions if necessary