CS 6378-Spring2023 – Software Security

Project: Design of a Secure Healthcare System

The healthcare system provides services for patient care and communication between patients and a clinic. The use cases are described below.

Your team must design a secure healthcare system to protect the system and sensitive data from threats or attacks. The secure health care system defines a security policy that outlines security requirements. On top of the security policy, your team needs to identify additional threats and provide security measures.

Security policy:

- The system shall be available except for maintenance hours.
- The system shall not disclose patient data to unauthorized parties.
- The system shall not violate the privacy of patient data.
- The system shall control employees' access to critical use cases.
    - A nurse or doctor can access the Record Visit use case.
    - Only a doctor can access the Treat Patient use case.

The following describes the instructions for designing a secure healthcare system.

System Boundary:

1. Define the system boundary using a software system context model that shows how the system interfaces with the external environment. Develop the threat model for the software system context model, where threats are identified and analyzed. Also, specify the security use cases to mitigate the threats and develop test cases for the use cases.
    a. Authentication use case: Use 2-factor authentication and apply time limitation to enter the second credentials.
    b. Check DoS attack: Avoid Bot's service requests and block the IP address requesting continuous requests.

Software Requirements:

2. Identify and analyze threats to each use case to develop the secure use case model. Specify the security use cases to mitigate the threats and indicate where the security use cases extend the application use cases using extension points. Develop test cases for the application use cases and security use cases.
    a. Need to identify two threats in each use case if possible.

3. Develop the class diagram that shows the entity and interface classes for application use cases and security use cases specified in (1) and (2). Indicate security classes among the classes with a stereotype. Apply threat modeling to the class diagram to identify additional threats.

4. Develop the secure interaction model that realizes each application and security use case, where the model needs to integrate application and security objects. Apply threat modeling to the secure interaction model to identify and analyze additional threats. Integrate new security objects against the additional threats into the secure interaction model. Develop test cases for the secure interaction model if the test cases differ from those created in (1) and (2).

Software Architecture:

5. Develop a secure (client-server) software architectural model that shows secure subsystems and their interactions. Identify and analyze additional threats to the software architectural model and provide security measures against the threats. Integrate the security objects for the security measures into the secure software architectural model.

Make your assumptions as necessary

Use Case Description for secure healthcare system:

Use case name: Make Appointment
Summary: The staff makes an appointment.
Actor: Staff
Precondition: The staff has logged in.
Main sequence:
1. Staff enters a doctor's name with whom a patient wants to make an appointment.
2. System displays a doctor's available date and time.
3. Staff enters the patient's appointment information (name, date of birth, and appointment date and time) if a doctor is available on a date and time.
4. System stores an appointment with the patient's name, phone, doctor's name, date, and time.

Alternative sequence:
- Step 3: If a doctor is unavailable, the staff exits or goes to step 1.

Postcondition: The staff has made an appointment.

Use case name: Check-in Patient
Summary: The staff checks in a patient.
Actor: Staff
Precondition: The staff has logged in.
Main sequence:
1. The staff enters the patient's name and date of birth into the system.
2. System displays the patient's appointment information if the patient has an appointment.
3. The staff selects the patient.
4. System displays the patient information (name, address, phone number, SSN, pharmacy, and health insurance) on the patient's medical chart if the patient is a returning one.
5. The staff enters the patient information into the system if it needs changes.
6. System updates the patient's information.

7. System marks the patient as ready to see a doctor.
8. System deletes the patient appointment.

Alternative sequence:

- Step 2: If the patient has no appointment, the system displays "no appointment" and exits.
- Step 4: If a patient is new, the staff enters the patient information, and the system creates the patient medical chart and then goes to step 7.
- Step 5: If there is no change, the staff selects the patient and goes to step 7.

Postcondition: The staff has checked in a patient.

Use case name: Check out Patient
Summary: The patient pays the medical fee for the visit to the doctor.
Actor: Staff, Patient, Bank
Precondition: The staff has logged in.
Main sequence:

1. The staff enters the patient's name.
2. System displays the patient's medical fee for the date's medical examination.
3. System activates the card reader.
4. The patient swipes a credit card for payment.
5. System requests a bank to approve the payment. If the bank approves payment, the bank returns a reference number to the system.
6. System updates the patient payment information.
7. System prints a receipt.

Alternative sequence:

- Step 4: If the patient pays with a debit card, the patient swipes a card and enters a PIN.
- Step 5: If the bank denies payment, the system goes to step 4.

Postcondition: The patient has paid the medical fee for a visit.

Use case name: Record Visit
Summary: Nurse updates patient chart with physical measurements and reason for the visit.
Actor: Nurse
Precondition:
Main sequence:

1. The nurse enters the patient's name.
2. System displays the patient's medical chart.
3. The nurse enters the patient's weight, height, blood pressure, temperature, and reason for the visit.
4. System updates the patient's medical chart.

Alternative sequence:
Postcondition: The nurse has recorded a patient visit.

Use case name: Treat Patient
Summary: The doctor treats the patient.
Actor: Doctor, Pharmacy
Precondition: The nurse recorded the patient visit.
Main sequence:

1. The doctor enters the patient's name.

2. System displays the patient's medical chart.
3. The doctor enters treatment content and a prescription if any.
4. System updates the patient medical chart.
5. System sends the prescription to the patient's pharmacy electronically if the doctor has prescribed medicine.

Alternative sequence: None.
Postcondition: The doctor has treated the patient.

Use case name: Ask Questions
Summary: The patient asks questions about their health issues.
Actor: Patient
Precondition: The patient has logged in.
Main sequence:

1. The patient selects "Ask Questions."
2. System displays the doctor, nurse, and staff names.
3. The patient selects a doctor, nurse, or staff.
4. System displays a blank page.
5. The patient writes a question.
6. The patient submits the question.

Alternative sequence: None
Postcondition: The patient has asked questions.

Use case name: View Lab Test Results
Summary: The patient looks at the lab test results.
Actor: Patient
Precondition: The patient has logged in.
Main sequence:

1. The patient selects "Lab Test Results."
2. System displays the dates that the patient had tested.
3. The patient selects a date.
4. System displays a test result to the patient.

Alternative sequence: None
Postcondition: The patient has looked at their lab test results.

Use case name: Request Refill
Summary: The patient requests refills from a doctor.
Actor: Patient
Precondition: The patient has logged in.
Main sequence:

1. The patient selects "Request Refills."
2. System displays the medications that the patient takes.
3. The patient selects medications to refill.
4. System displays information about the medications.
5. The patient submits the medications.

Alternative sequence:

- Step 5: If the patient selects "Cancel," the system exits.

Postcondition: The patient has requested refills.