# COM6003 – Threat Modelling

This document will provide an overview of the approach taken to identify, assess and mitigate security threats that could potentially affect the security and functionality of the Hospitality management application. The areas in which this document will cover consists of keys assets such as user credentials, patient data, staff data, appointment details and system configurations and protocols.

This document will also go into detail about the potential threats the system might face, how they will affect the system, the mitigation strategies used to prevent potential threats as well as a matrix to visualise the impact and likelihood of a threat.

Key Assets

* User Credentials – User credentials are one of the most important assets within a secure system storing sensitive data as they are used for authentication and authorization of functions within a system and also the ability to gain access to a system, user credentials consist of –
  + Usernames and Passwords – Used for primary authentication, in this case logging in and connecting to the system. These credentials must be stored securely using strong hashing algorithms.
  + Multi-Factor Authentication Tokens – Used to provide an additional layer of security, ensuring only authorised user can access sensitive data.
* Patient Data – Patient data is the centre of a hospitality management app, covering all information relating to patients within the system such as –
  + Personal Identification Information – This consists of names, addresses, phone numbers, emails, government ID numbers.
  + Medical History – Contains patient diagnoses, treatments, medications, allergies and previous medical procedures.
  + Sensitive Health Information – This includes lab results, imaging report, blood sample results and consultation notes.
* Doctor Data – Information related to medical professionals within the hospital system. This data is critical to the functionality of the hospital system, necessary for appointment scheduling and providing patient care. This data consists of –
  + Schedules – Availability and work hours of doctors to manage appointments and surgeries.
  + Contact Information – Phone numbers and email addresses to contact doctors internally and in the case of emergencies.
  + Specialities and Qualifications – Information about a doctors area of expertise, their qualifications and certifications.
* Appointment Details - Appointment Details contain scheduling information that connects patients with doctors and departments within the hospital. This data includes –
  + Patient Doctor interactions – Details about previous visits and the outcomes, as well as upcoming appointments including dates, times and the purpose of the visit.
  + Appointment Status – Information regarding the status of an appointment and whether is has been rescheduled, cancelled or complete.
  + Resource Allocation – Information regarding the room bookings, equipment needed and the personnel assignments.
* System Configuration – System configuration data and logs are vital to tracking the activity within the system and monitoring the system for inconsistencies and breaches, this includes –
  + Configuration Settings – Includes system parameters, user permission levels and network settings.
  + Audit Logs – Logs of user activities, access attempts and system events that provide traceability.

STRIDE Threat Analysis

* Spoofing – Unauthorised access by impersonating legitimate users –
  + An attacker using stolen credentials to log in as a doctor or administrator
  + Phishing attacks to trick users into leaking legitimate login credentials
  + Mitigation strategies –
    - Implementing Multi-Factor Authentication makes it harder for unauthorised users to gain access to sensitive data by providing an additional layer of security
    - Enforce strong password policies such as, minimum 8-character length, must include both upper and lowercase letters and well as at least one number and symbol. On top of this periodic password changes help the overall security of the system.
    - Education on potential cyber attacks and the methods hackers may use to gain access to the system
* Tampering – Unauthorised modification of data within the system –
  + An attacker editing patient records to falsify medical information
  + Modifying appointment schedules to create confusion and disrupt the systems and services
  + Mitigation Strategies –
    - Enforce Role-Based Access Control to ensure only authorised user can perform specific actions
    - Use Cryptographic hashing to verify data integrity and detect unauthorised changes
    - Implement audit logging to track all changes made within the system, flagging unauthorised changes and providing traceability
* Repudiation – Users denying having performed actions within the system –
  + A staff member denying that they made changes to a patients record
  + An attacker attempting to cover their tracks when tampering with patient records
  + Mitigation Strategies –
    - Implement action logging with time stamps and User ID to provide a clear audit log of all actions made within the system
    - Use digital signatures for critical actions
* Information Disclosure – Unauthorized access to sensitive data –
  + An attacker intercepting data sent between the app and the user
  + Unauthorized users accessing patient records due to incorrectly setup permissions
  + Mitigation Strategies –
    - Encrypt data while in both transit and storage using strong encryption algorithms
    - Implement access control to restrict access to data based on the user’s permission roles
* Elevation of Privileges – gaining higher access privileges than intended –
  + A receptionist taking advantage of a vulnerability to gain administrative permissions
  + An attacker exploiting misconfigurations within the system to gain access to restricted areas of the app
  + Mitigation Strategies –
    - Use the principle of least privilege, ensuring that users always have the minimum access level necessary to their role

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Impact | Likelihood | Rick Level |
| Spoofing | High | High | High |
| Tampering | High | Medium | High |
| Repudiation | Medium | Medium | Medium |
| Information Disclosure | High | High | High |
| Elevation of Privilege | High | High | Medium |

In Conclusion, due to the nature of the application, being that it holds sensitive information not only for the patients of the hospital but data around the people who work there. Due to this there are a large number of security risks, however, with the correct implementation of the mitigation strategies these risks can me managed and the security of the application can be maintained.