## The Problem Description

Queens medical center is a clinic that serves patients in various areas of medicine by specialists, the patient needs to get an appointment for a consultation meeting with the specialists, the scheduled appointment is done by using a telephone call to the center receptionist.

The clinic is facing a high volume of calls, which affected the residents to get the care on time, also, the clinic management has a plan to respond to the increase in population in their community.

## The solution

The management of the clinic decided to get an online system to manage the appointments, which is a web-based system for appointment and scheduling management information system (ASMIS).

## The benefits of ASMIS

ASMIS has advantages such as:

* Saving time
* 24/7 Available
* Reduce no-shows
* Reduce empty slots
* Reduce administrative work
* Effective information management

ASMIS will solve the problem which affects the residents causing by a high number of calls, in addition, the system will succeed to overcome the problem with the growth of the community population by saving the time and effort of meeting scheduling.

## Understand the risks

In the Internet era and converting toward the digital business, in addition, the concerns about the high rate of cyberattacks and the government’s policy about patient data protection, there is a need to install electronic online appointment and scheduling system. however, the system should be secured and guarantees privacy. The system collects vital information about patients, therefore, exposing patient data privacy or confidential health data must be prevented by the system otherwise, Queens medical center will violate privacy laws and will face legal punishment.

## Objective

Install a secured system (ASMIS) by optimizing network security and using threat modeling to recognizing targets, potential threats, and vulnerabilities in the system. After that providing a mitigation plan for those threats which is the most effective security solution for the system.

According to (Alhassan et al., 2016) threat is anything that causes the malfunction of the system or the provided services or leads to patient data disclosure and compromising system confidentiality, integrity, and availability.

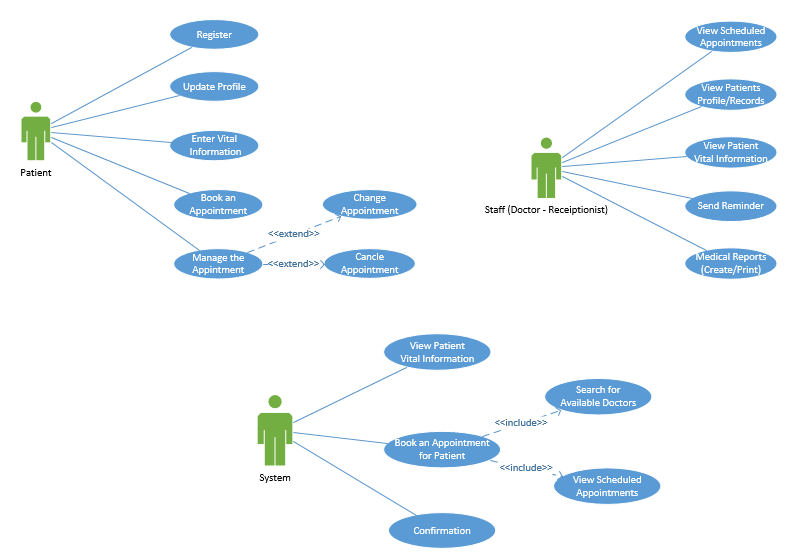
## Software security approach

Required three factors (security requirements – threat modeling – threat assessment)

## security requirements

At the first, defining the actors of the system and the main components which need to be protected.

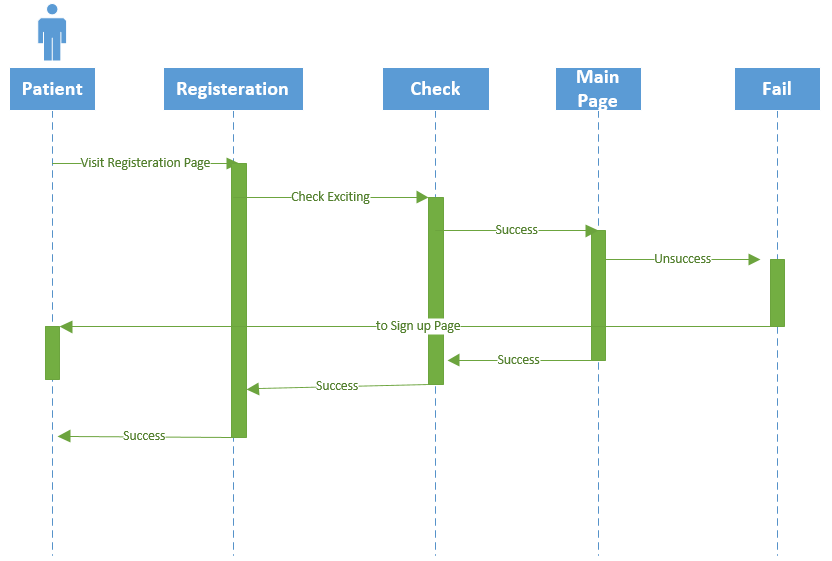
Actors: Patient, Staff such as (Specialist doctors, Receptionist, Finance …etc.), and the System itself.

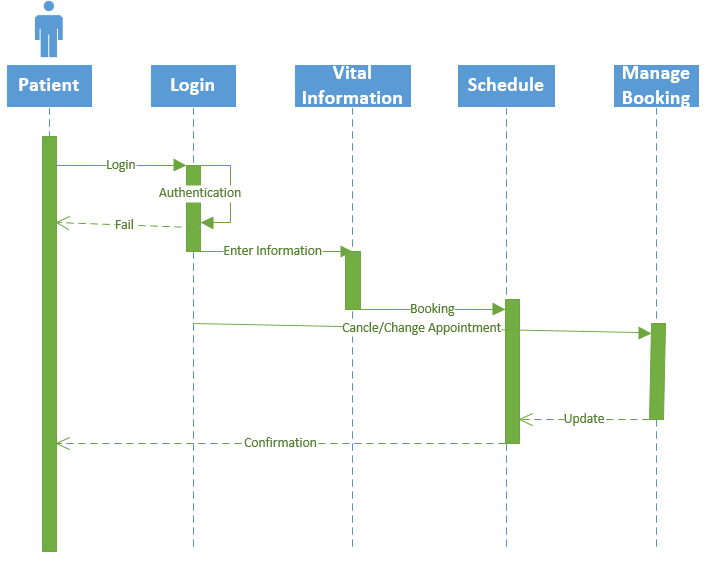


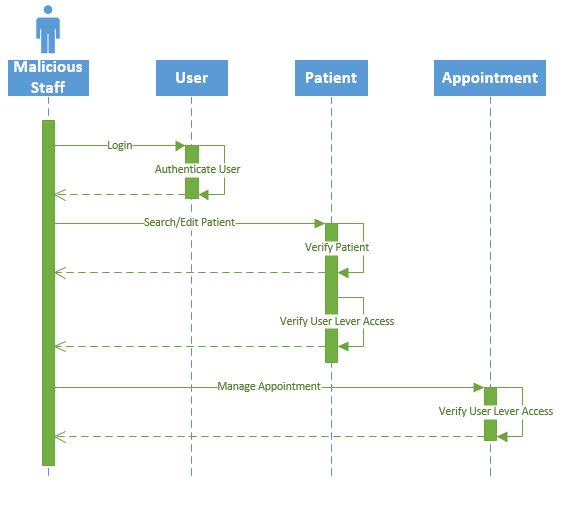
*Figure 1: ASMIS Actors Use case*

To illustrate the system function and structure for ASMIS, will use class diagrams and sequence diagrams as shown in the next diagrams.









*Figure 2: ASMIS class diagram and sequence diagram*

The patient starts with browsing the Queens Medical Center web page. Then, register as a new profile or login if he has one. After the successful login, he must enter his vital information such as patient status and symptoms to make the system able to decide the best doctor for his case. Then, the system will search for the available specialist and check the doctor's schedule time. Finally, according to the patient case, availability, and workload of the doctor, the system will book an appointment with the patient and send him the confirmation.

The receptionist or system can send a reminder to the patient to remind him about his appointment. Patients can manage their appointments by cancel or change and the appointments will be scheduled easily.

The specialist doctor can search and retrieve patients' records, view patients’ vital information and medical history, search the scheduled appointments, search reports, and prescribe medicines for patients.

For the ASMIS system, need to protect the web-based application, Hardware such as (Servers, Networks, and Communications), Power source, and Patients Data and Appointments which are saved in the Database. This essay will focus on the most important part which is to protect patients' data/Information.

Patient records should not be accessed, updated, and deleted by an unauthorized user. In addition, the scheduled appointment should not be updated by change date, time, and doctor or deleted by users unless done or requested by the patient himself. The system will send the confirmation for the created appointment or changed one.

Information saved in the ASMIS system includes personal information such as names, phone numbers, emails, addresses, and age, in addition to vital information and medical history which are protected by privacy law. Therefore, the key risk for ASMIS include:

* loss of patient’s personal data.
* loss of patient’s confidential data such as medical status.
* Compromise patient data.
* Denial of Service attacks, which affect the availability of online appointment services.
* Reputational damage.

## Threat modeling

According to (Abomhara et al., 2015) threats may come from inside or outside the system, from authorized users who have authorized access to the system, or from unauthorized users.

Threat modeling is an analysis of the potential threats which violating the CIA triad model Confidentiality, Integrity, and Availability of Patient’s data. This essay will use the STRIDE model to classified potential threats.

Modeling threat for ASMIS system, four key steps are needed, include assets identification, access points identification, threats identification, and identified threats rating (Alhassan et al., 2016).

**Assets identification:** valuable component for the system or organization, which may attract the attacker, or in other words some things that we need to protect (Abomhara et al., 2015).

In the ASMIS system, which is an appointment and Scheduling online system, the assets are the system itself, Database, and users. The assets value ranges from high to low, therefore, the ASMIS system’s assets are Network Infrastructure, Database, web-page application, and users as the following diagram. Patients and Users connect to the system through the webpage.

Patient data, User’s data, and appointments are stored in the database. Patients visit the web page to get an appointment and enter their vital information which is stored in the database, users such as doctors access the database to search patients’ information and check the scheduled appointments.



*Figure 3. ASMIS assets*

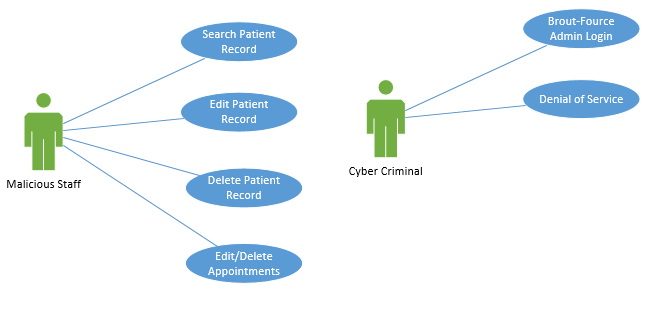
**Access Point Identification**: points where attackers may use to get access to the assets such as login interface, ports, configuration files, and open sockets (Alhassan et al., 2016). After that, setting trust boundaries such as network boundaries, user privilege level, and access rights.

**Threat Identification**: it known as threat modeling, it is important to finding threats and system vulnerabilities, which helps to measure the cost and impact of those threats on the system or actors, in addition, helps to mitigate those security risks. For ASMIS system will use the STRIDE model for the threat identification process.

STRIDE model classified threats into six categories as following:

* **Spoofing**: attempting or act to gain unauthorized access using a fake identity, this security risk aims at **Authentication**.
* **Tampering**: modification or changing of data done by unauthorized access, this risk concern with **Integrity**.
* **Repudiation**: the ability of legitimate or illegitimate users to deny that performing of action or event, this concern with clearing system logs.
* **Information** **Disclosure**: data breaches or confidential information is exposed or leaked; this risk aims at **Confidentiality**.
* **Denial of service**: action makes System, Application, Service, or Network unavailable; this attack aims at **Availability**.
* **Elevation of Privilege**: authorized users with limited privileges gain access to higher-level privileges, threat aims at **Authorization**.

Using of STRIDE model to identify threats on the system actors or assets, which violate authentication, integrity, privacy, authorization, and availability of system, service, or data.



*Figure 4. ASMIS threats*

Appling STRIDE mode on the ASMIS assets as following tables:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Assets | Threats | | | | | |
| S | T | R | I | D | E |
| Patient | S |  | R | I |  | E |
| Staffs |  | T | R | I |  | E |
| Database |  | T |  |  | D |  |
| Web page |  |  |  |  | D |  |

|  |  |  |
| --- | --- | --- |
| Authentication Threats | | |
| Description | STRIDE | Assessment |
| Patient credentials loss or sharing | Spoofing | Low |
| Staff credentials loss or sharing | Spoofing | High |
| Patient credentials theft and misuss | Elevation of Privileges | Medium |
| Staff credentials theft and misuss | Elevation of Privileges | Medium |

|  |  |  |
| --- | --- | --- |
| Authorization Threats | | |
| Description | STRIDE | Assessment |
| Unauthorized Access to system data | Elevation of Privileges | High |
| Unauthorized access to admin functionality | Tampering - Elevation of Privileges | High |
| Patient modify data after getting over privileges | Tampering | Low |
| Staff modify data add or delete | Tampering | High |

|  |  |  |
| --- | --- | --- |
| Privacy Threats | | |
| Description | STRIDE | Assessment |
| Patient Data Disclosure | Information Disclosure | High |
| Staff Data Disclosure | Information Disclosure | High |

|  |  |  |
| --- | --- | --- |
| Auditing and Logging Threats | | |
| Description | STRIDE | Assessment |
| Patient deny receiving confirmation or edititng appointment | Repudiation | Medium |
| Staff deny updating or deleting data | Repudiation | High |

|  |  |  |
| --- | --- | --- |
| Availability Threats | | |
| Description | STRIDE | Assessment |
| Web page not accessible | Denial of service | High |
| Database not accessible | Denial of service | High |

## Threat Assessment

In the previous tables in threat modeling, threat assessment classified threats into high, medium, and low according to the impact and likelihood as shown in the following figure.



*Figure 5. Threat Assessment Matrix (Pivot Point Security, 2016)*

## Threat mitigation and countermeasure

The final step is to make a proposal for how to mitigate the threats which are identified in the threat modeling step.

(Cagnazzo et al.,2018) declared that authorization threats could be prevented by using a strong authorization framework and privacy threats could be prevented by using reliable encryption techniques, moreover, a combination of authorization and encryption could achieve security aspects such as integrity, authenticity, liability, and trust; protecting Denial of Service attacks which affects availability with deep packet inspection filtering system.

(Alhassan et al., 2016) highlighted that using biometric authentication is better than traditional password-based authentication, could not be lost, shared, easy to guess, and easy to break, in addition, it can prevent repudiation and integrity threats, alongside applying user authorization levels and restricts users to access only his function group will prevent fraud and conflict of interests by putting a barrier between groups; in addition, making attack discoverable by applying digital forensic technique; to protect the database from DoS and tampering threats using cryptography technique, data redundancy, and digital forensic techniques.

(Abomhara et al., 2015) proposed mitigation plan and countermeasures related to each group of threats as following: for spoofing threats, strong authentication, encryption, and cryptographic protocol such as TLS/SSL should be applied; strong authorization, data hashing and signing, and securing communication links could prevent tampering threats; to mitigate repudiation threat using secure audit trails; while could encountering information disclosure threats with strong authorization, encryption, secure communication links techniques; finally, applying the principle of least privileges helps to mitigate elevation of privilege threats.

(Möckel & Abdallah, 2010) provided some mitigations such as avoiding social engineering attacks by creating user awareness and using password generators instead of simple passwords to mitigate spoofing threats; prevent tampering threats by using firewalls between web server and database to stop direct access and applying sophisticated access right level; using comprehensive logging process to mitigate repudiation threats; to overcome information disclosure with applying protocols such as TLS/SSL and HTTPS protocol for the web-based platform; moreover, prevents Denial of Service threats by system performance testing, backup system, and plan for emergency and business continuity; protecting elevation of privilege threats through two-factor authentication technique.

For Queens Medical Center system (ASMIS), regarding the above studies, threats could be mitigated as following: authentication threats which are done by spoofing patients and users, and elevation of privilege on patient and user credentials can be prevented by using strong authentication such as multi-factor mechanism and strong password policy; alongside with applying encryption technique to ensure that all credentials should be encrypted before transmission; applying protocols such as TLS/SSL and HTTPS to encrypt the communication. To prevent elevation of privilege threats by applying strong authorization techniques such as least privileged account and separation of user group depending on their functions and duties. Tampering threats such as modifying or deleting data by patients or users could be prevented by using a strong authorization mechanism with the least privilege and separation group, using digital signature and hashing mechanism to ensure that data is valid, and securing communication links alongside installing a firewall between web server and database. Privacy threats that aim toward information disclosure such as patient and user data disclosure could be mitigated by strong authorization and encryption mechanisms such as check access right before allowing access to data and service and encryption all sensitive data before storing them in the database. Repudiation threats where patients or users may deny receiving or updating data while the system could not prove that has happened, such as threats could be prevented by using logging for all activities and transactions in the database, in addition, securing log files by restricted access control lists. Availability threats such as Denial of Service attacks which may affect Database and web page by using firewalls and proxies, backup system, and load balancer.

## References

Abomhara, M., Køien, G. & Gerdes, M. (2015) ‘A STRIDE-Based Threat Model for Telehealth Systems’, *NISK Journal (2015)*. November. 82-96. Available from: https://www.researchgate.net/publication/291766457\_A\_STRIDE-Based\_Threat\_Model\_for\_Telehealth\_Systems [Accessed 8 October 2021].

Alhassan, J., Emmanuel, A. & Olaniyi, O. et al. (2016) ‘Threat Modeling of Electronic Health Systems and Mitigating Countermeasures’, *International Conference on Information and Communication Technology and Its Applications*. Minna, Nigeria, November. 82-89. Available from: https://www.researchgate.net/publication/311238739\_Threat\_Modeling\_of\_Electronic\_Health\_Systems\_and\_Mitigating\_Countermeasures [Accessed 4 October 2021].

Cagnazzo, M., Hertlein, M. & Holz, T. et al. (2018) ‘Threat modeling for mobile health systems’, *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE. 314-319. Available from: https://ieeexplore.ieee.org/document/8369033 [Accessed 2 October 2021].

Möckel, C. & Abdallah, A. (2010) ‘Threat modeling approaches and tools for securing architectural designs of an e-banking application’, *2010 Sixth International Conference on Information Assurance and Security*. IEEE. Available from: https://ieeexplore.ieee.org/document/5604049 [Accessed 3 October 2021].

Pivot Point Security. (2016) Why Use Matrix-Type Models for Risk Assessment?. Available from: https://www.pivotpointsecurity.com/blog/using-matrix-models-for-risk-assessment/ [Accessed 8 October 2021].