Issues of the calling system.

The Queens medical center has been trying to find ways to manage the high volume of calls. The ASMIS has been introduced as the online platform with the issues to handle the appointments and especially the urgent ones with the specialists on time. To understand why the ASMIS is important, we must understand why it was implemented. The main reasons that this management information system has been created, was firstly to deal with the high volume of calls by prospective patients who would like to book an appointment with a specialist. On top of this, the secretary had to check the availability and the workload of the specialists and based on it, to book an appointment at the earliest convenient of both the patient and the specialist which was really a time consuming procedure. Furthermore, the patients could book an appointment only during the opening hours of the clinic.

Benefits of ASMIS.

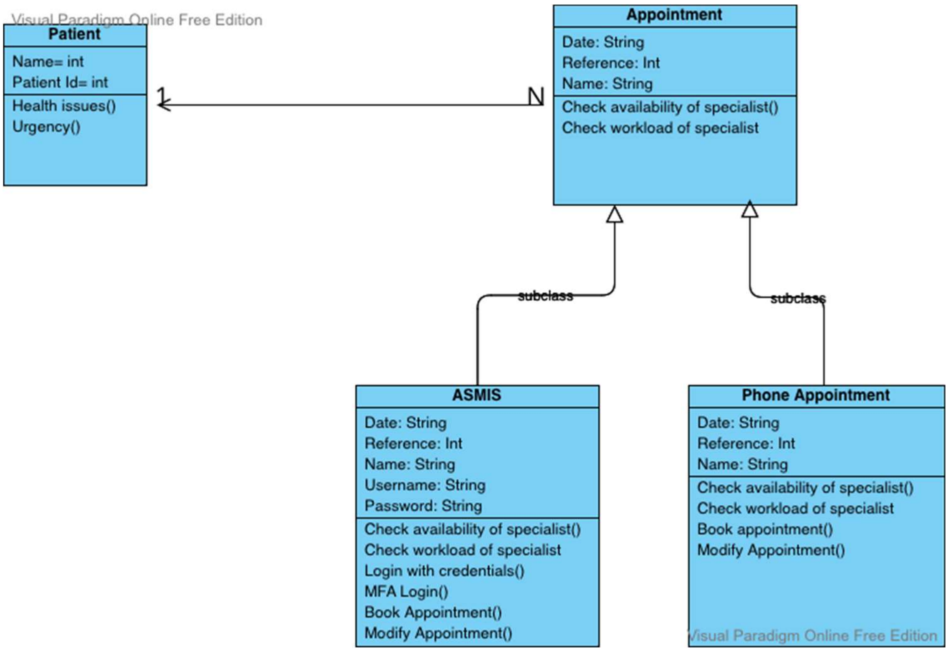
This is where the ASMIS comes to solve the issues mentioned above. First of all, it solves the high volumes of calls. The ASMIS replaces the tasks of the secretary and allows the patients to book an appointment with a specialist instantly. Secondly, it gives the opportunity to select a favorite specialist at an available date bypassing the secretary. Additionally, the patients can use the booking system at anytime compared to calling the clinic that is available only during the opening hours of the clinic. Furthermore, the medical record of the patient is saved in the ASMIS database which allows every specialist to consult it and make a better diagnosis about the patient issue. This will also allows him to manage his appointment and possibly adjust the dates of his appointments. In addition, the ASMIS allows the patient and his specialist to consult his/her previous consultations, consult his/her medications and even consult his/her family record. Finally, it provides a login function with MFA authentication.

Problems with ASMIS

The ASMIS like every other management system has to deal with the potential cyber threats that include the Malware and Ransomware attacks, Denial of service attack, the phishings, MITM, the social engineering attacks and the account take overs. Concerning the ASMIS the Ransomware or Malware can cause unauthorized access to the Queens clinical management system, and modification of the health patient medical record. In addition, it can cause unavailability or system failure of the system as well as stealing the credentials of the patients with unauthorized access and taking over their accounts using phishing and social engineering, MITM methods by taking advantage of the elderly age of the patients and their nativity.[1][3][4]

Diagrams

ASMIS Class diagram



Background information to the ASMIS class diagram

Patient class

Patient class has a relationship 1 to N with Appointment class

Patient attributes includes the Name and the Patient id.

Patient operations include the Health issues and the Urgency

Appointment class

Appointment class includes the following attributes: Date, Reference, Name and the following operations: Check availability of specialist and Check workload specialist

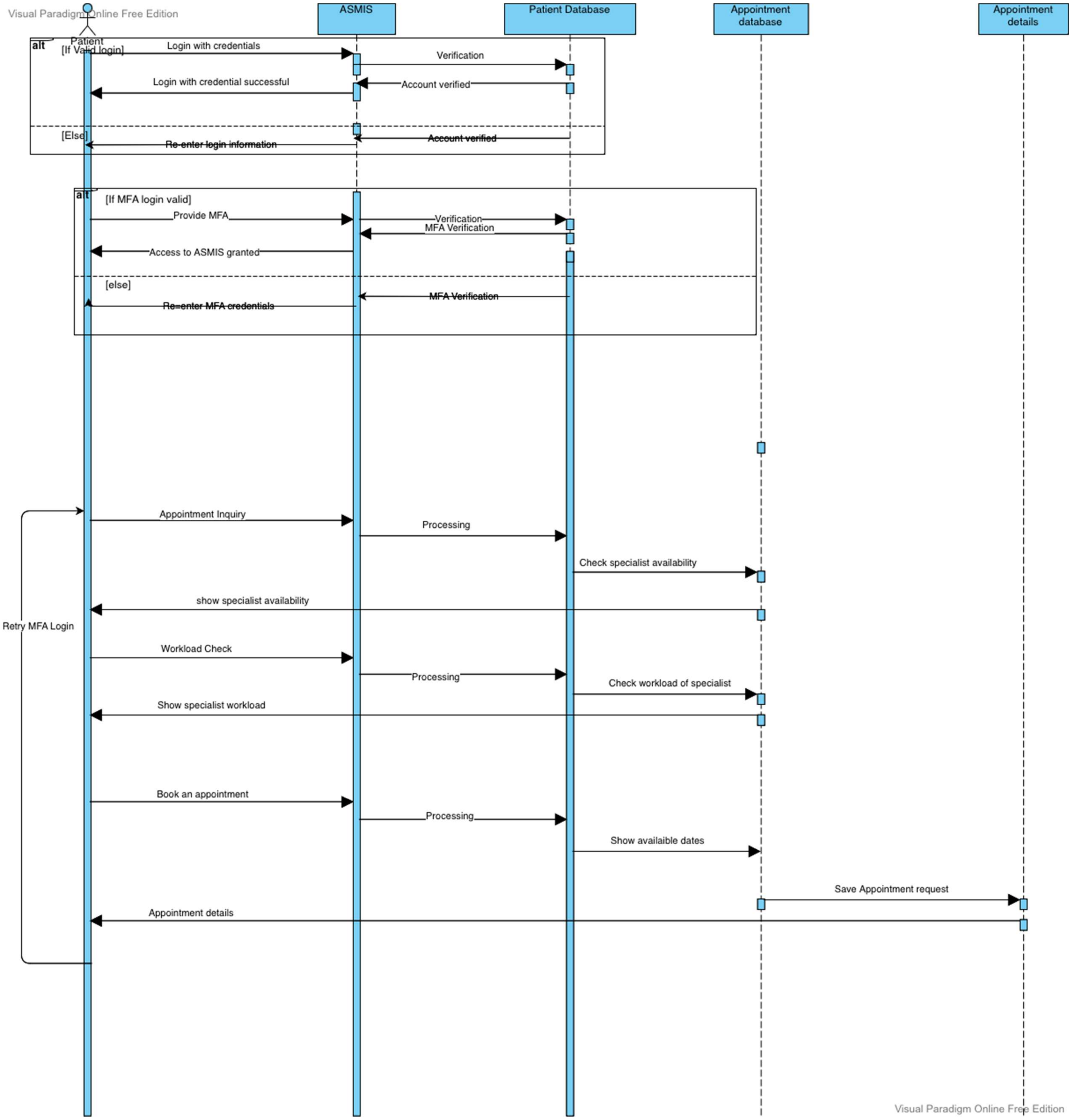
The appointment class is extended by the following two subclass that copy the attributes of the Appointment class.: ASMIS and Phone system appointments.

Subclasses: ASMIS and Phone Appointment

The ASMIS extends the appointment class with these extra attributes username and Password and the following extra operations: Login with credentials(), MFA Login(), Check specialist availability(), check specialist workload(),Book appointment(), Modify appointment().

The Phone appointment extends the appointment class with these extra operations: Check specialist availability(),check specialist workload(), Book appointment(), Modify Appointment().

ASMIS Sequence diagram



Background information of the ASMIS sequence diagram

Step 1: Request: Login to the system providing valid credentials- 1st authentication.

Response: If validation fails retry step 1. Else If it succeeds, move to step 2

Step 2: Request: Login to the ASMIS with MFA – 2nd authentication

Response:Proceed to step 3 if valid. If invalid return to step 3.

Step 3: Request: As patient check the specialist availability via the ASMIS.

Response: ASMIS returns the specialist availability.

Step 4: Request:Patient check the workload of the specialist.

Response: ASMIS returns the workload of the specialist

Step 5: Request: Patient Books an appointment via the ASMIS

Response: ASMIS books an appointment and saves the patient details in the ASMIS database and return appointment details to the patient.

Cyber threat models

The potential issues that might occurs with the ASMIS can be described using the two popular cyber threat models: the STRIDE and the DREAD cyber threat modelings.

STRIDE stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege.

Stride mitigates to the ASMIS as following.

- Firstly by allowing unauthorized access to the ASMIS such as using a similar erroneous URL that directs the patient to other website (Spoofing),
- Secondly, by modifying important information of the health patient record using spywares, Trojan horses, or even relay attacks (Tampering),
- The ASMIS should be able to trace all possible access to the system and allow the patients using the system to trace any access not performed by them (Repudiation),
- Revealing information to unauthorized people like profitable organizations must be refused. This means that the ASMIS should be able to react to the following threats: Phishing, sniffing, Man in the middle, path traversal, compromised key, wifi eavesdropping, ransom-wares and predictable paths locations (Information disclosure),
- Unavailability to the system which means that the patient will not be able to even book critical appointment at Queens clinic (DDoS).
- Gaining access as a hacker while being unauthorized. STRIDE can take care of the following elevation of privileges adware's, worms and Luring attacks (Elevation of Privilege). [2]

DREAD

The DREAD was implemented by using categories to estimate the rating of a threat.

Dread stands for **D**amage, **R**epuducibility, **E**xploitability, **A**ffected users, **D**iscoverability.

There are thee ratings 0,5,10 which correspond to 1, 2 and 3 level accordingly. DREAD can be mitigated to the ASMIS as following

- Damages will analyze the seriousness of the attack to the ASMIS
- Repuducibility will analyze if the attack to the ASMIS is repeatable and how is should it be to repeat this attack to the ASMIS.
- Exploitability will indicate how easy it will be for a hacker to attack the ASMIS
- Affected users are obviously the patients of the Queens Clinic, as well as the medical staff who will not be able to consult the ASMIS to make a proper diagnosis
- Discoverability should show how easy a cyber attack can be detected in the ASMIS.

To better understand the DREAD cyber threat model some the following table was created to explain in a few words why the DREAD model is ideal to rate the risk of the cyber-threats.

The values bellow rate the risk for each of the elements described above.

10 = high risk, 5 = medium risk, 0= low risk. [5]

Questions	Answers
How much damage does it to do the ASMIS?	0= No damage. 5= Medium damage. It displays only minor information of the patients. 10= It damages all the patients using the ASMIS.
Is it possible to reproduce the Cyber-attack to the ASMIS?	0= Impossible. 5= Reproduce it as administrator. 10= Run it without user account.
Is it easy to perform an Cyber-attack to the ASMIS	0= Very difficult 5= Only experienced hackers. 10= Everybody can run the attack.
Who is affected by the Cyber-attack to the ASMIS	0= No patient. 5= Patients with weak credentials. 10= All the patients.
Is it easy to discover the Cyber-attack to the ASMIS	0= Almost impossible. 5= Only experience developers can trace the attack. 10= Novice users can discover that the ASMIS was hacked.

Cyber security technology

The Queens medical clinic has to find some ways to deal with the cyber threats to protect the patients' confidential information due to the cyber attacks and the government policy on patient data protection. The main focus of this report is the efficient, user friendly and secure authentication that allows the patients and medical staff to safely access the ASMIS. Taking into consideration the CIA triangle, the following cyber security authentication methods are selected to secure the ASMIS: SSL certificate with SHA-1 encryption, biometric authentication, single sign-on, and multi- factor authentication (MFA).

1. SSL certificate with SHA-1 encryption.

   As authentication, it uses SSL certificate with SHA-1 encryption for overall site secure data exchange and one-way SHA-1 hash for secure data exchange. Moreover, it also uses SHA-1 hash on all passwords, with encrypted password saved in the database, no information of the patient patient are stored except of the email address of the patient. It also requires a strict username/password format. Finally, the recovery of the password includes a four-point password retrieval system such as the Full name, date of birth, last 4 digit of NN and answer successfully to three security questions.

   On the other side, the SSL with SHA-1 encryption does not provide anymore sufficient encryption as it used to be when it firstly appear because it has a lot of cryptographic weaknesses. In addition to this the SHA hash was not accepted by many application and as a result, it was discontinued. An example of this technology was my Health e-link used by Riverside, Regional medical centre.

2. Biometric authentication

   The patients and the medical staff can install an application configured by the administration team of the clinic in combination with biometric authentication.

   The benefits include that it is a method based on encryption using distinctive physical human characteristics such as Iris, fingerprint or voice authentication or fingerprint reader.

   On the contrary there are major issues with reverse engineering. The Imprivata One sign authentication management is an example of this method.

3. Single Sign-on.

   The patients and the staff login to a computer in combination with the usage of a badge or fingerprint and a unique password.

   The benefits are the following: OneSign Authentication Management, it is secure with a No Click Access, it provides fast access to the ASMIS, it allows to log in using a fingerprint or a badge in combination with unique password, it helps the patient to avoid memorizing multiple password, finally it is the primary stage to assist the patients by gathering in one place extensive information of care experience. The Bio-key Healthcare security represents this technology.

4. Multi factor authentication (MFA).

   A user can successfully be authenticated in the ASMIS by using two of the following three factors: Firstly, the knowledge factors such as the date of birth, credentials and National security number. Secondly, possession factors such as token devices, smartphone, phone call backs, or other smart devices. Finally, things that only the user knows such as answering to questions like favorite pet, middle name of mother, first car, etc.

   The benefits of MFA include: Additional security authentication, supports mobile devices, reduce frauds and identity thefts, decrease operating costs, promote transactions, simplify login process and enhance customer trust.

   However, it is important to consider the following drawbacks such as that the difficulty to back up or migrate the credentials, issues with the integration with smartwatches, the major issues with MITM attack and the loost or the theft of the device. An example of this is duo-API which is supported by Android and Apple mobiles. [6]

Conclusion.

To sum up, taking into consideration the cyber security technologies described above, the SSL certificate with SAH-1 encryption seems not to be widely supported by all the systems which might be a risk for the ASMIS to integrate and it misses as well security encryption protocols . In addition to this, the biometric authentication as a standalone method is subject to reverse engineering and in combination with social engineering can allow the hacker to gain access to the ASMIS.

However, despite its disadvantages, the most efficient, widely used and most secure way to reduce the cyber threats is the Multi factor authentication. It is also highly suggested to use it in combination with the single Sign-on method in special circumstances such as for the experienced medical staff and the elderly patients that are hospitalized in the clinic because it allows fast, and convenient access to the ASMIS of the Queens clinic.

References:

1.Judo, S. (2019) Evaluation of threat modeling methodologies. Jamk university of applied science. Available from: https://www.theseus.fi/bitstream/handle/10024/220967/Selin_Juuso.pdf?sequence=2&isAllowed=y [Accessed on 19 November 2022]

2. Khan, S.A. (2017). A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security. *International Journal of Computing, 05*, 13-20.

3. Pavlik, L. (2018). Identifying and Modeling the Impact of Cyber Threats in the Field of Cyber Risk Insurance. *2018 5th International Conference on Mathematics and Computers in Sciences and Industry (MCSI)*, 118-121.

4. Lella. I & Tsekmezoglou, E. & Svetozarov, R.D. & Ciobanu, C.& Malatras, A. & Theocharidou, M. (2022) European Union Agency for Cybersecurity 2022. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport [Accessed on 16 November 2022]

5. Simula , A. (2015) Security risk and health models for health care product development processes. Jamk university of applied science. Available from: https://core.ac.uk/download/pdf/38131677.pdf [Accessed on 16 November 2022].

6. Tipton, S.J., Forkey, S. & Choi, Y.B. (2016)Toward Proper Authentication Methods in Electronic Medical Record Access Compliant to HIPAA and C.I.A. Triangle. J Med Syst 40(4): 100. https://doi.org/10.1007/s10916-016-0465-x