This assignment looks to introduce a web based appointment system within a health care clinic and to ensure that this system is not only fit for purpose but is also secure. The following report will look at the advantages and disadvantages of implementing such a system, including a visual representation of the system through behavioral and structural diagrams. The report will then apply a security framework to identify potential risk of cyber attacks. Any device that is connected to the internet has the possibility of being vulnerable to a cyber attack. Therefore the report will also look at mitigating these risks using security technology.

Below is a list of benefits of implementing a web-based appointment system for the clinic:

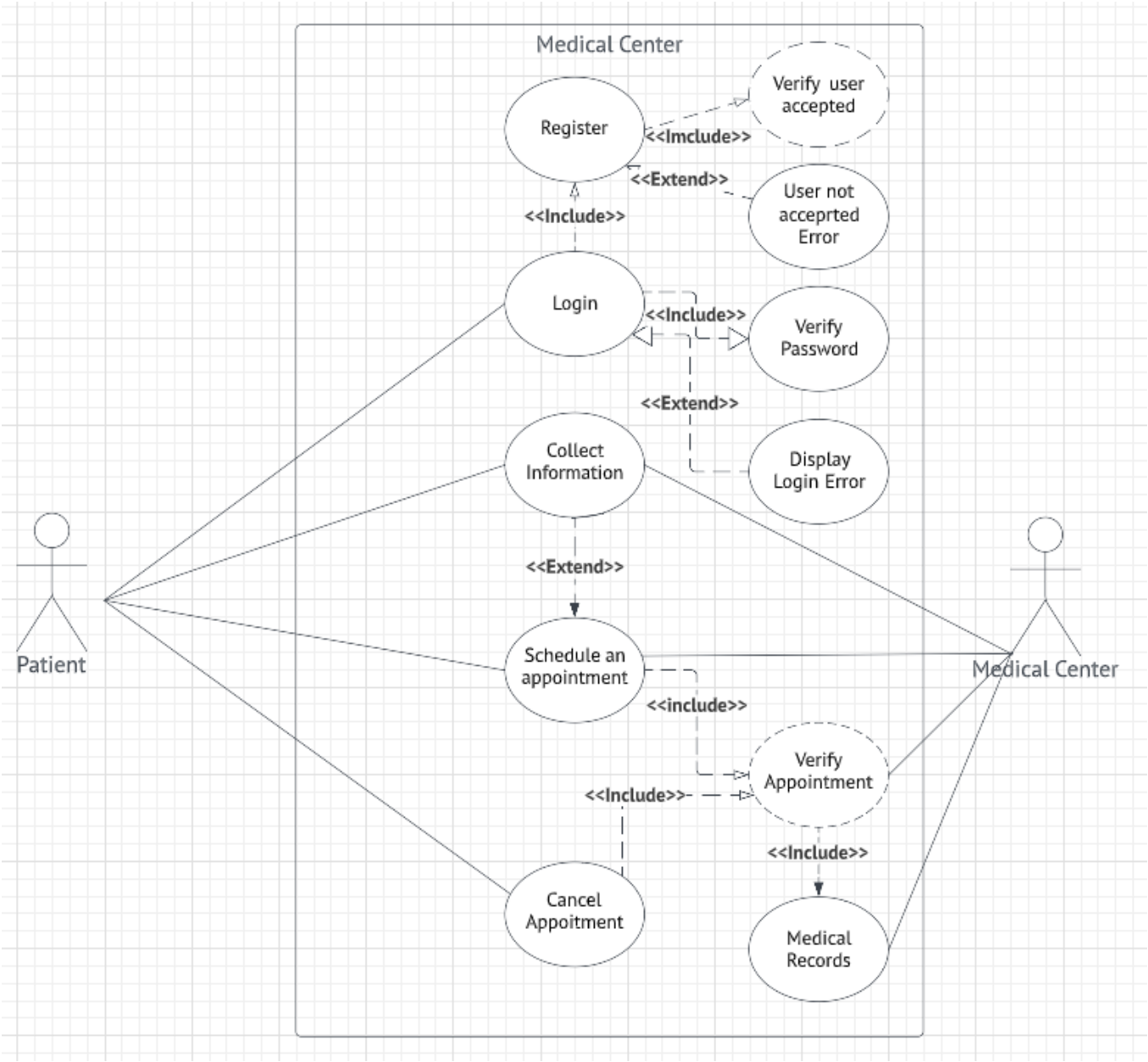
- Patients are not restricted to making enquiries only by telephone.
- Any waiting time or back logs during busy periods are reduced.
- As this is web-based, it is easy to access and does not require patients to download any software.
- Potential human error is reduced.
- Appointments will now be updated in real time which will allow doctors to view their own schedules.

The following is a list of disadvantages of implementing a web-based appointment system:

- If an ISP (Internet Service Provider)  or mobile device have connectivity issues, then booking an appointment will not be possible.

- Many patients (especially the elderly) may not have the technical knowledge necessary to access the system.
- If the clinic itself is having system issues, doctors will not be able to access their schedules and therefore will not be able to retrieve any patient details.  This could cause a serious problem in case of an emergency.
- Having a booking system online leaves you more at risk for a potential cyber attack.

Using tools such as use case, class and sequence diagrams increase the awareness of the flow of the system. Below is my first behavioral diagram, a Use Case Diagram. This explains the basic flow of the systems and introduces the system users (both internal and external) to the system.

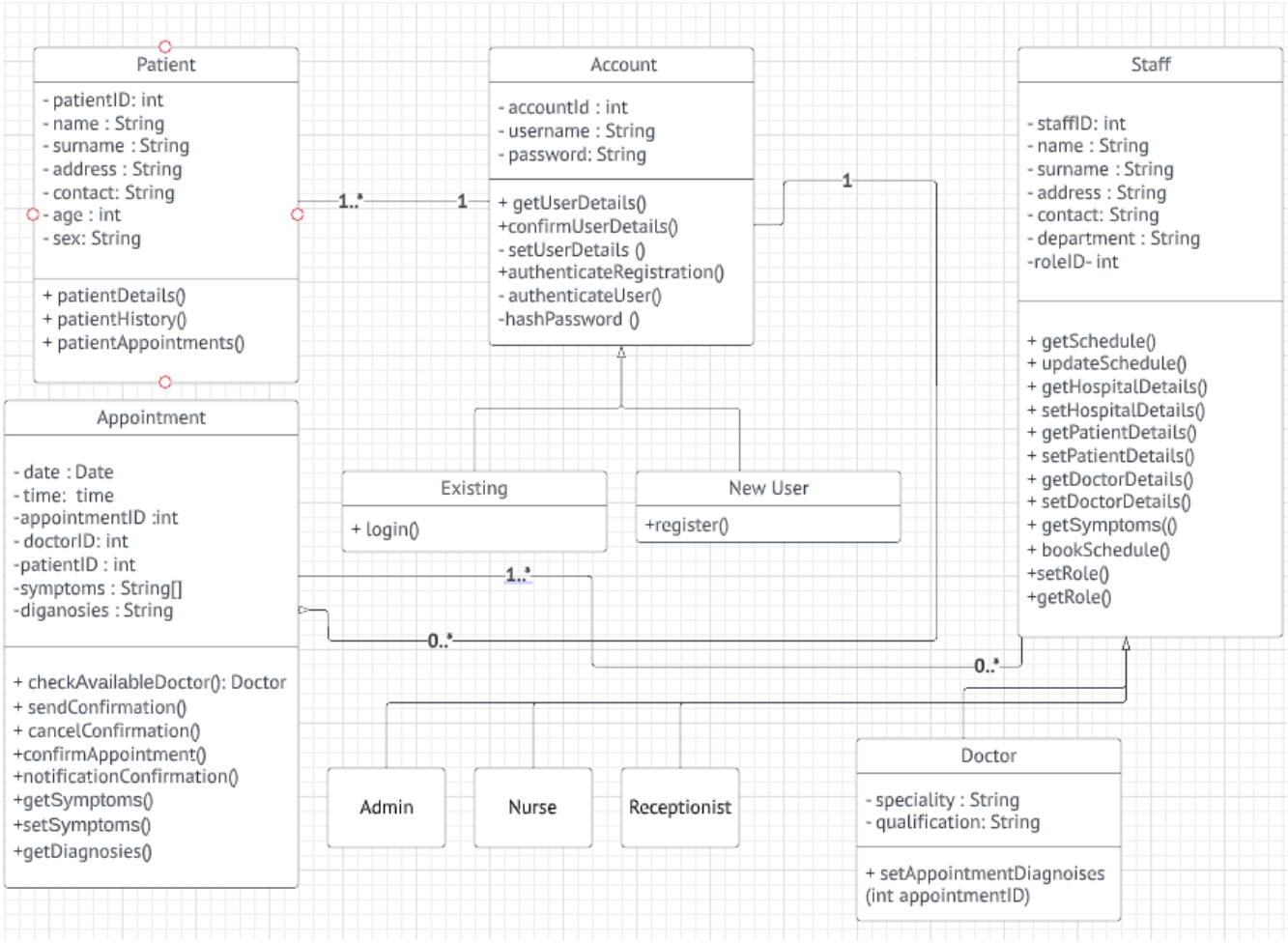



Use Case Diagrams 1.1

- The actor's of the system will be patients who live within the specified catchment area.
- If the patient is not already registered within the system, they will need to register. During this registration process, the patient will need to provide proof that they live within a predefined catchment area. Once confirmed, they will be able to proceed with logging in.

- If the patient has registered previously they will need to provide a username and password which will be verified before access to the system is granted.
- Once the patient has successfully logged in, they will be required to select the symptoms they are currently experiencing. They will be asked a list of questions with multiple choice answers and they will need to select the answer(s) that best fits the symptoms they are experiencing.
- Once the symptoms have been submitted, they will be cross referenced against a Database. The Database includes a list of all the available specialists at the clinic and their specialist areas including symptoms they commonly treat. The system also includes a schedule, which can determine if a specialist has any availability to see a patient.
- Once a specialist has been assigned to a patient and an appointment has been booked, the patient will have to verify the appointment to confirm.
- Once the booking is confirmed, the patient's medical records will be sent to the doctor in real time.

The class diagram is a structural diagram, which represents a blueprint of classes and objects and clearly maps the object name with its attributes and operations. It provides an overview of the inheritance of the parent and child class and shows the relationship of classes of the overall system. This also specifies the scope of the object with the access modifiers such a private, public or static.
[UML Class Diagram Tutorial, n.d.]



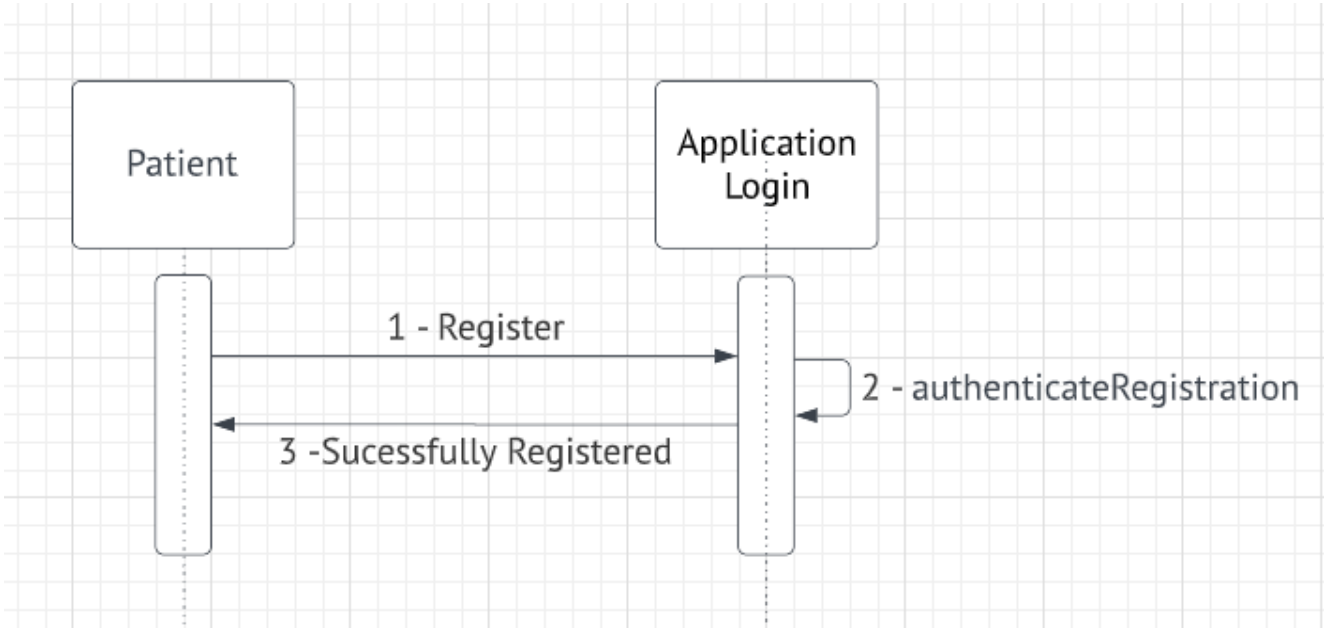
Class Diagram 1.1

- A patient class may have a one to many relationship with an Account. This is to ensure that anyone under the age of 18 has an adult present during the appointment.
- Account can have a one to many relationship with the Appointment class. This ensures that a patient can see many specialists however only have one appointment at a given time.
- Staff Class has a zero or many to one appointment relationship. This is to factor in that there may be no appointment on a given day or there may be many that the staff need to attend.
- Staff class is an abstract class for Admin, Nurse, Receptionist and Doctor.

- A User Account is a parent class which comprises of an Existing or New User class. Depending on the class invoked the appropriate method will be provided.
- Admin, Nurse, Receptionist and Doctor are all child classes to Staff.
- All attributes have been kept private so that the class is only able to access them.
- Getters and setters have been created, that will ensure that retrieving the data is only available via the getters, while the setter allows for modification.
- The parent user Account class consists of a username (string) and accountID (integer) to give a unique value and a password. Depending on the action the user will inherit either invoke login or register method.
- The password will be a hashed password and kept in the database, so no one is able to view it.
- The Account class has a method called authenticateUser, which will be private, so only available to the class.
- Staff members will have access to different patient data depending on their job role and level of seniority. Please note that I have included various staff roles such as admin, nurse, receptionists and doctor. The permission allocated to each of these individuals will be role dependent, which will be set by the Stafff class using getRole and setRole.
- Doctor has an additional method called setAppointmentDiagnoises, which takes an integer value of appointmentID so the doctor can update the records and ensure privacy to the patient id.

The sequence diagram is my second behavioral diagram, which captures a high level flow between the actors (patient ) and systems. Here the essence is to capture the lifeline (the dotted line) which represents the start to the end of each process, as well as the active period of communication with the process (which includes data going back and forth) represented by vertical rectangles.

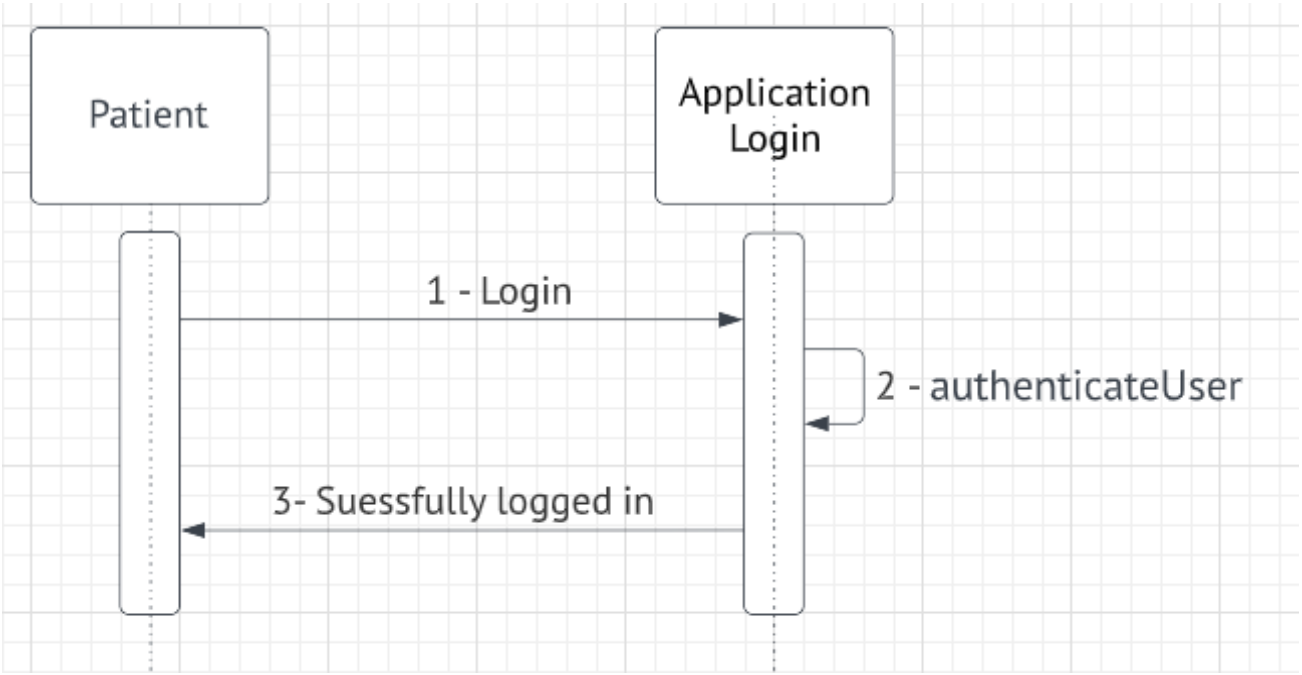
[What is a sequence diagram in UML?,  n.d.]




Sequence Diagram 1.1

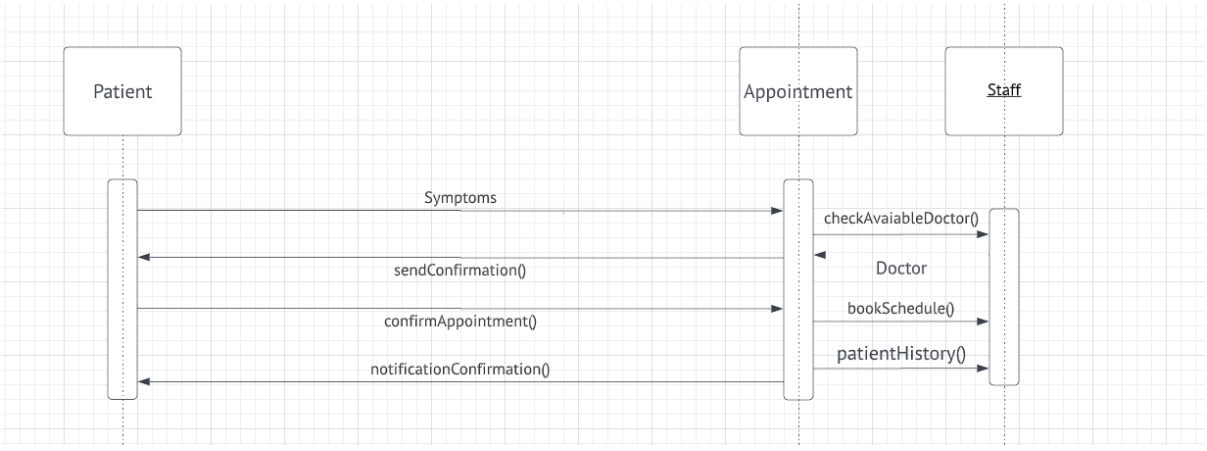
- Any New user will need to register and provide personal information
- This data is then processed and validated to determine if the user is granted permission to access the system.
- A return message will be displayed to the user confirming if the registration has been successfully completed. If the registration has not been successfully completed, there will be no reason given why registration has not been approved, in order to not compromise existing user data.  Instead users will be directed to contact the clinic directly.

- Once registration is successful for a new user, they will need to log in. This will initiate the communication.




Sequence Diagram 1.2

- An existing user will need to log in.
- This data is then processed and validated to determine if the user is granted permission to access the system.
- A return message will be displayed to the user confirming if the login has successfully completed. If not successful the users will be directed to contact the clinic directly.




Sequence Diagram 1.3

- Assuming the users have logged in successfully, they will then be required to select their symptoms.
- The schedule will invoke checkAvaiableDotor method, which determines a good match by reconciling the doctors specialty, doctors availability and the patients' symptoms.
- The schedule will receive a return object of Doctor with details of the specialist doctor they are matched with as well as the time and date of the given appointment.

A framework is also needed to identify potential risk and threats that may occur during the lifetime of the system One such framework is STRIDE, a threat modeling tool and an acronym which stands for 6 security risk categories, which are:

- Spoofing - This identifies risk with authorisation and determines if login credentials of users are being used by someone else to log into the system.
- Tampering - This prevents unauthorised modification of data.
- Repudiation - This ensures if a security breach occurs this can be proven and traced.
- Information Disclosure - This ensures that sensitive data is not exposed to individuals who are not authorised to access the data.
- Denial of Service - This attack stops users from being able to use the system.
- Elevation of Privileges - This threat identifies if someone has been able to access something or perform something that they should not have the authority/ permission to do.

This tool allows you to analyse the system for each of the above security risks and determine the threat and the impact of that risk whilst offering suggestions to what line of defense should be used.

[Peeple, K, 2015]

The below STRIDE 1.1 table is divided into each of the STRIDE categories with the associated description of the attack, the likelihood of the attack occurring, the impact to the system, and the countermeasures to avoid such a situation.

STRIDE 1.1 table

| STRIDE | Description | Likelihood of this event | Impact to the system | Mitigation / Countermeasures. |
|---|---|---|---|---|
| Spoofing | An attacker trying to impersonate a user and logging in to the system | High | High | • Strong Authentication<br>• Password policy<br>• Ensure data is encrypted<br>• Multi Factor Authentication |
| Tampering | users accessing unauthorised data by modify, delete to update records | High | High | • Ensure role based access control is in place for systems and authorised areas<br>• Using multi factor authentication |
| Tampering | Data Modification when data is in transit | High | High | • Ensure data is encrypted using protocols such as the SSL, TLS HTTPS |
| Repudiation | Not knowing if system has been attacked | High | High | • Ensure audit logs are captured for all |

| | | | | |
|---|---|---|---|---|
| | | | | activities of the system |
| Repudiation | Log files being tampered with | High | High | • Ensure the disaster recovery site also maintains backup and replication |
| Information Disclosure | Staff who do not have direct contact with a patient being able to view patient information(Third party disclosure) | High | High | Ensure role based access control is in place for systems |
| Information Disclosure | Clear text being displayed during network packet transfer | High | High | Ensure communication is all via secure |
| Information Disclosure | An attacker manipulating or retrieving the data from the Database (Also known as SQL injection.) | High | High | Access control |
| Denial of Service | User unable to communicate with the system due to large amount of data traffic | Low | High | • This is a tricky one to determine if this is actually a threat or a pandemic outbreak and if the requests are genuine. In this scenario it would be advisable to review over a period of time and to set up a disaster recovery so if an attack has taken place, or if the system is overwhelmed a disaster recovery can |

| | | | | |
|---|---|---|---|---|
| | | | | be introduced on a different network segment<br>• Increase the network bandwidth<br>• Create a DOS response plan<br>• Practice good cyber training |
| Elevation of Privileges | Staff deleting or misusing patient details. | | | • Ensure all staff have a role based access control, with least privileges as default<br>• If any task needs to be performed, there should be an audit trail to indicate the time, access applied for and who authorised it.<br>• Only senior members can provide approval |

The following section will discuss the cyber security technologies that are required. The report first looks at the type of network layer attacks then application layer attacks. I identify possible solutions and discuss the advantages and disadvantages of these solutions.

Network Protection

To ensure the network is protected, we need to look at securing it with hardware devices like a Firewall. We aso need to ensure that we use secure ports. There are a number of Firewalls available, such as Packet Filtering, Proxy firewall, software based Firewalls or GNFW (Next-Generation FireWall). This technology has evolved and is more secure than the traditional Firewall as it includes Intrusion Detection and protection. The advantages of using a Firewall is that you have an additional layer of security protection, blocking malicious traffic like viruses and hackers.

[Bonuccelli, 2020]

A major disadvantage of utilising a Firewall is that some vendor products can be very costly. A firewall can also obstruct some activities within the organistion such as sending images or attachments. There can also be network delays as the firewall would need to analyse all packets being transmitted. Having a Firewall in place will also require a dedicated team to monitor and tune the firewall policy. Finally there is no guarantee that this will stop the system from being hacked.

Secure Protocols

When using Internet protocols, we need to ensure that we are not using insecure methods such as HTTP (HyperText Transfer Protocol) which uses plain text to transfer data. Instead we should be using only HTTPS (HyperText Transfer Protocol Secure) which uses port 443 opposed to port 80. This will ensure secure communications are sent via TLS (Transport Layer Security) a method of encryption that provides both privacy and data integrity. important factor is that it also ensures that any attempt to tamper with the packets will be detectable.

[What is SSL?, n.d.]

The key advantage of using an Internet protocol is that data travels through HTTPS and is always encrypted. If a hacker was to intercept the data, it would be hard to decrypt. All data sent via HTTPS is validated before the transfer occurs. The disadvantages are that there is a yearly cost to purchase a certificate, and performance of the system is likely to be delayed as all data needs to be encrypted and decrypted.

Application Protection

To prevent attacks such as SQL injection and XSS from occurring, we need to ensure any statements from the application are using binding parameters, these will act as place holders for when executing the code. We also need to ensure that access rights are used to access the database such as a RBAC (Role-Based Access Control).

[Zhang,E, 2020]

The advantages of using binding parameters is that we limit the interaction from the User Interface limiting the attackers to what sql statement can be entered. Additionally, with least access right we ensure the data can only be modified or deleted by an authorised person. The major disadvantage of binding parameters is that we can only limit symptoms to a drop down list and therefore may miss some key symptoms that patients are experiencing from this list. The disadvantages of RBAC are that we are only able to wait for selected users who can perform data patch.

To prevent authentication attacks, we need to ensure we implement strong passwords including letters, uppercase, numbers and special characters. We also need to ensure any email address and contact details hold the special characters such as @ and .com.  Another authentication factor is to apply 2FA (two-factor authentication) which ensures the user trying to log in is actually who they say they are.

[Why multi-factor authentication is an essential part of cyber security, 2020]

The advantages are that there will always be another layer of security to ensure the password is not hacked. The disadvantage is that these two factor authentications increase login times as you now need to enter a password and then an additional verification is needed. Additional disadvantages may include costs of hardware to ensure we can send SMS messages or tokens are synched to allow access. This hardware will also need maintenance and likely a team to support customer complaints.

This assignment has been a great learning experience and it has taught me that security should be considered during the design phase of any new project to ensure a system can defend itself from an attack. However, once the system has been implemented, it is essential that security should continue until the end of the lifespan of the system.

REFERENCE :


Allen, J(n.d.)
Privilege Escalation Attacks: Types, Examples, And Prevention Available from:
https://purplesec.us/privilege-escalation-attacks/

bbc.com(13 May 2017)
Cyber-attack: Europol says it was unprecedented in scale. Available from:
https://www.bbc.com/news/world-europe-39907965
[Accessed 28 April 2022]

Bonuccelli, G (November 4, 2020)
What Are the Basic Types of Firewalls? Available from:
https://www.parallels.com/blogs/ras/types-of-firewalls/
[Accessed 11 April 2022]

Donovan, F (January11, 2021)
What is STRIDE and How Does It Anticipate Cyberattacks? Available from:
https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/
[Accessed 14 April 2022]

Get Cyber Safe(February 17, 2020)
Why multi-factor authentication is an essential part of cyber security Available from:
https://getcybersafe.gc.ca/en/blogs/why-multi-factor-authentication-essential-part-cyber-security Available from:
[Accessed 10 April 2022]

Lucidchart.com(n.d)
UML Use Case Diagram Tutorial Available from:
https://www.lucidchart.com/pages/uml-sequence-diagram
[Accessed 28 April 2022]

Peeple, K(02 December 2015)
STRIDE Threat Model Available from:
https://dzone.com/articles/stride-threat-model#:~:text=Repudiation%20threats%20are%20associated%20with,to%20trace%20the%20prohibited%20operations.
[Accessed 27 April 2022]

SSL.com(n.d.)
What is SSL? Available from:
https://www.ssl.com/faqs/faq-what-is-ssl/
[Accessed 27 April 2022]

UML Class Diagram Tutorial from:
https://www.visual-paradigm.com/guide/uml-unified-modeling-language/uml-class-diagram-tutorial/

[Accessed 24 April 2022]

Zhang,E (1 December 2020)
What is Role-Based Access Control (RBAC)? Examples, Benefits, and More  Available from:
https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more
[Accessed 28 April 2022]