Cybersecurity Technologies for Web-Based Appointment Scheduling and Management Information System

Launching into Cybersecurity

NOVEMBER 20, 2022

UNIVERSITY OF ESSEX

Contents

[Summary 2](#_Toc119940186)

[Introduction 2](#_Toc119940187)

[Benefits of web-based appointment and management information system (ASMIS): 2](#_Toc119940188)

[Discussion 2](#_Toc119940189)

[Potential Cyber threats to the web-based appointment and management information system (ASMIS): 2](#_Toc119940190)

[● Phishing: 3](#_Toc119940191)

[● Ransomware Attacks: 3](#_Toc119940192)

[● Data Breaches: 3](#_Toc119940193)

[● Denial of Service Attacks: 3](#_Toc119940194)

[UML Diagrams: 3](#_Toc119940195)

[Threat Modelling Techniques: 4](#_Toc119940196)

[Cybersecurity technologies and its strengths and weaknesses: 5](#_Toc119940197)

[● DNS Firewalls: 5](#_Toc119940198)

[● Authentication and Authorisation: 6](#_Toc119940199)

[● Secure Web gateway (SWG): 6](#_Toc119940200)

[Conclusion 6](#_Toc119940201)

[References 8](#_Toc119940202)

# Summary

The purpose of this report is to propose a solution to the existing problem of appointment bookings and management of Queen’s medical centre, a community clinic for the residents of the catchment area and the primary point of contact when someone happens to fall sick. The Queen’s medical centre is facing a high volume of calls for appointment booking and are unable to respond to all residents culminating in lack of access to the care. Also, an increasing growth in the population size of the area poses additional concerns in regards to the existing scheduling system. The management of the centre has come up with a plan to install a web-based appointment and management information system (ASMIS) for booking online appointments whereby the system would gather certain information necessary to book appointments as per doctor’s availability and caseload. The purpose of this report is to identify cyber threats and create a secure ASMIS through using security technologies to mitigate the risks.

# Introduction

## Benefits of web-based appointment and management information system (ASMIS):

Businesses that instigated online booking systems generated 37% growth in the revenues. Furthermore, 79% of the service users like to book and reschedule appointments online. (Samuel, 2022) The web-based appointment and management system is a convenient and secure way of booking appointments in healthcare settings as it has various advantages. Booking appointment requires the service users to click on the designated URL by the service provider such as healthcare organisations and fill in the requested details that most commonly is followed by an email or SMS alert for the completion and booking of the appointment.

ASMIS can have myriad numbers of benefits. Firstly, it saves time taken by the staff to book appointments for the patients over the phone. Every call would take several minutes to just book the appointments hence reducing the productivity of staff that in presence of ASMIS would divert their time in essential activities. Secondly, the reduction in extra human resource would help the companies to monetise money and reduce the expenses. Thirdly, with the online booking option, people can schedule their appointments anytime round the clock. Fourthly, all the data about the patient is stored in a centralized information system which makes it easy to access by both patient and the staff. All the vital information can be accessed by healthcare professionals reducing the need to duplicate information multiple times. (Sanjana, 2019) Lastly, the online booking option provides flexibility to the users to access the service from any place at any time and as per their convenience. (Hakim, 2022)

# Discussion

## Potential Cyber threats to the web-based appointment and management information system (ASMIS):

On average, UK healthcare organisations in a week experience almost 785 cyberattacks. In general, the healthcare sector is fronting a 69% increase in cyberattacks. (Serena, 2022) There are several potential cyber threats to the healthcare sector including online appointment booking systems. Data is crucial for any healthcare organisation but poor security infrastructure and lack of investments in the security technology of this valuable information attracts the cyber attackers to exploit the vulnerability. Following are the potential cyber threats to the web based appointment and management information system.

### Phishing:

Phishing is the most prevalent cyber threat in the healthcare industry. (Edward, 2022) Phishing emails look genuine and authentic and requests for login details of the service user or the staff to get the login credentials for easy access in the system. Different viruses planted with the phishing email will either mine record data or leave the door open for the hacker for later. (CTI, 2019)

### Ransomware Attacks:

Ransomware attacks are commonly triggered by phishing attacks where hackers would ask for ransom after acquiring access to sensitive information. Cyber attackers are aware that industries like the healthcare sector where disturbances would result in massive damage would easily agree to the ransom. 1 out of 3 healthcare organisations fell prey to the cyber-attacks globally in 2020. (Edward, 2022)

### Data Breaches:

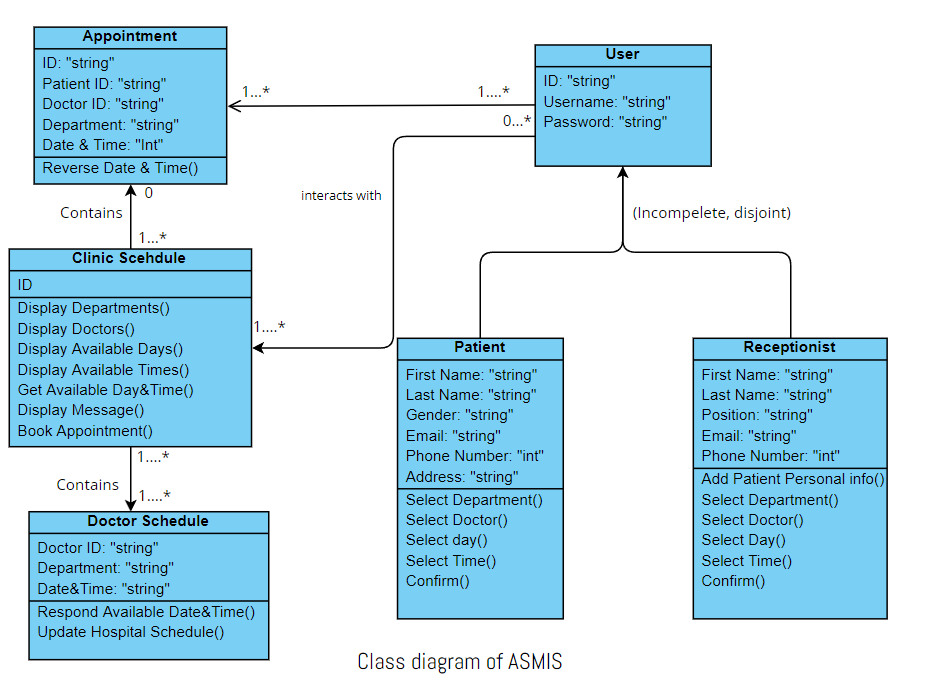
Healthcare entities suffer from more data breaches than any other sectors despite the fact that health insurance portability and accountability act (HIPAA) requires organisations to protect health records and sensitive information but the loopholes in security technologies let the attackers gain access. (Edward, 2022) These breaches can also be a result of staff leaving the data open to unauthorised use by others in their absence as well as third party vendors who provide staff without assessing the associated risks.

### Denial of Service Attacks:

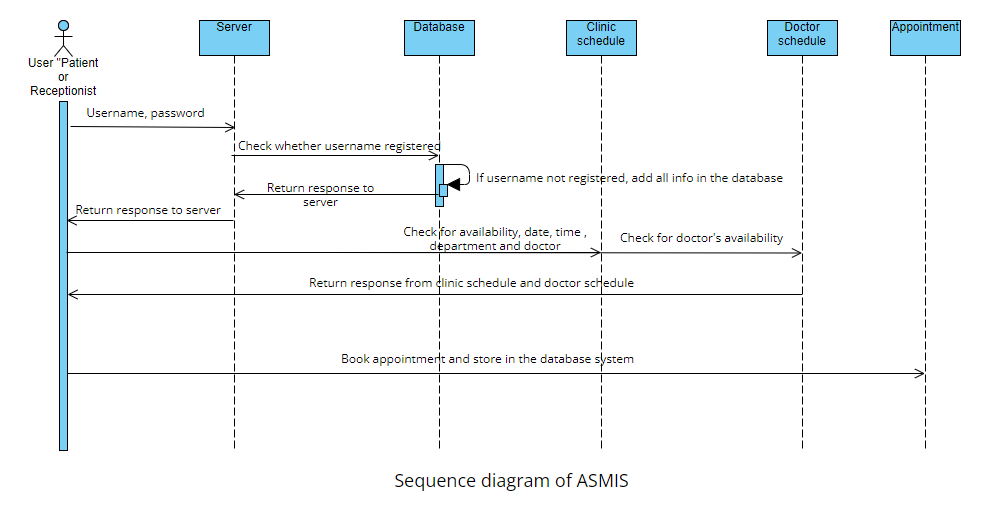
Web-based patient portals, electronic health records and medical resources for doctors can be used to easily target the organisation’s server and act as a database administrator to alter information. One such example is denial of service attack whereby the victim’s network is flooded with traffic resulting in denial of service which can culminate in damages to the organisation’s reputation and delays in access to care. (Richard, 2022)

### UML Diagrams:

Unified Modelling Language is a structured and rich language that helps in visualising, constructing and documenting new software systems and its blueprints. UML diagrams were created for the developers to solve complex problems and divide the problem into smaller components. UML is used to model new software, analyse the existing ones and plan the whole developmental process. (Miro, 2021) UML diagrams are broadly divided into two types, structural and behavioural. (creately, 2022). The following diagram shows the modelling of the proposed ASMIS based on two types of UML diagrams, first being from the structural type of UML diagram called “Class Diagram” and the other being from the behavioural type called “Sequence Diagram”. Both diagrams depict the relationship between different attributes in the system and their interaction. The class diagram below allows to display various classes such as appointment, User and clinic schedule etc. The attributes display information like ID, department, username name and passwords etc. that falls under the class. The operations are the functionalities such as reserve, confirm, respond and book etc.



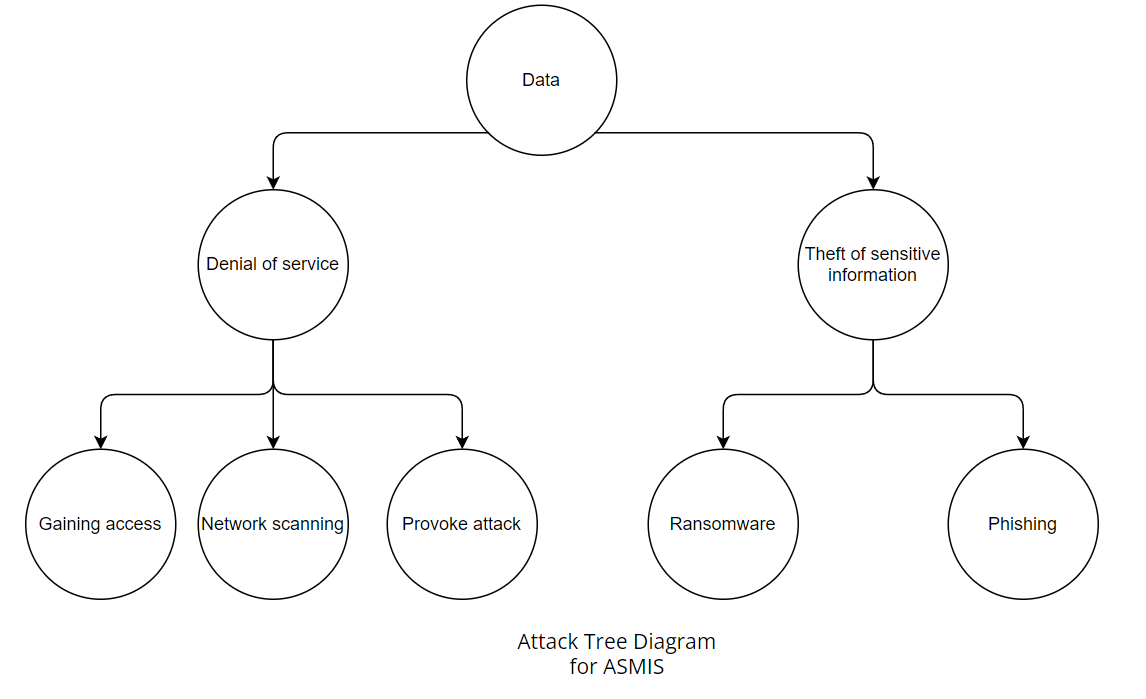
The sequence diagram as the name implies shows the series or steps of interaction between different elements. The below diagram represents the interaction between users, messages exchanged between the objects to perform a certain function.



## Threat Modelling Techniques:

Almost all systems today face some kind of threat and as technology advances the number of threats grows. Keeping in mind the risks and vulnerabilities of the system, it is necessary to analyse the threats side by side when building the system. Threat modelling techniques are essential in object oriented programming as they provide a vital step to access the threats collateral with developing a software. Threat modelling helps in identifying the abstraction of the system, potential attacker and their motives as well as potential threats. (Nataliya, 2018) Two of the threat modelling techniques that can be used to identify threats while developing the ASMIS system can be STRIDE and attack trees. The STRIDE method follows all the elements like spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges that makes it the most mature technique. Not all the elements in the STRIDE method are useful for ASMIS. Identifying spoofing is critical in the ASMIS as it is important to determine who is the genuine user and should be given access in the system. Tampering again is paramount as any changes in the system might expose the sensitive information related to the users or organisation. Information disclosure is an absolutely critical area and holds a lot of repercussions if the sensitive information leaks and violates the GDPR (general data protection regulation). Denial of service can serve as the biggest hit to an organisation and a halt in the healthcare sector can cause fatal damages.

Attack trees help to break each step of the potential attack and identify key goals, objectives, methods and assets in the attack. For attack trees in case of ASMIS, the potential goal of the attacker can be to get sensitive information like credentials, to get access to the system and demand for ransom. The sub steps are to identify the attack methods like phishing, ransomware etc. Keeping in mind the potential threats, it is essential to apply cyber security technology to mitigate the risks associated with the web-based appointment scheduling and management information system.



## Cybersecurity technologies and its strengths and weaknesses:

The key cyber threats identified in the previous sections need to be addressed with appropriate cyber security technologies to mitigate the risks and build a secure web-based appointment scheduling and management information system.

### DNS Firewalls:

The DNS firewalls help to filter traffic from DNS endpoints. It does this by checking the relationship between the web addresses and IP addresses and all the incoming traffic is checked against the policies. It is important to keep the addresses in the organisation up to date. Since in ASMIS, the users either patients or admin uses the web scheduling service hence its paramount to keep the addresses in sync. DOS (Denial of service) attacks can cause a great disruption in the scheduling of appointments in ASMIS hence implementing firewalls in the DNS layer can be an effective way to stop DOS attacks from happening.

Like every system, firewall has its disadvantages. It can be costly for certain organisation, can lower computer’s overall performance, can restrict users and it is not enough to protect from malware attacks.

### Authentication and Authorisation:

Authentication is the process to determine who the user is when using a system, in this case ASMIS. Asking a user for username and password is the first step in determining the authenticity of the user but is not enough to protect both the user and the system so it is paramount to introduce Multi Factor authentication like one-time password or biometrics to verify the service user. Authorization only allows access to certain permissible resources for the user. In ASMIS, it is important for every user of the system to be able to access the resources that are limited to their needs. For example, Patients should only be permissible to access their own portals. Similarly, Admin should only be able to access resources in their scope.

Authentication generally has more benefits than disadvantages. The first benefit is it improves the user experience and to use and adopt. It provides an extra layer of security. Authentication can protect users from brute force attacks when users have weak passwords. Also, it reduces the cost in the long run and simply to implement the technology. (Denis, 2018)

### Secure Web gateway (SWG):

Secure web gateway is modern cloud based security technology to protect users from malicious content over the internet by securing the endpoints. A cloud based secure web gateway works on the zero trust approach to protect the user by creating an additional layer to mitigate the risks as the user navigates through the internet, blocking known and unknown threats. (Jack, 2021) Secure web gateways incorporates the following features:

1. Web proxy
2. Policy enforcement
3. Malware detection
4. Traffic inspection
5. Data loss prevention
6. URL filtering
7. Sandboxing

SWG has various benefits like detection and prevention of threats, exposure of encrypted traffic threats, better visibility and monitoring and compliance with regulatory requirements like GDPR. (Vijay, 2021)

# Conclusion

The existing telephone based appointment system in Queens Medical Centre is exhaustive and overwhelming as per the growing needs of the community and hence a web-based appointment scheduling and management information system is crucial to reduce the burden on the system and provide timely care to its residents. Keeping in mind the aforementioned potential threats, modern cyber security technologies are needed to combat the attacks on the healthcare sector, which is facing an increasing number of cyber-attacks. It is important as a cyber-security professional to understand every step in object oriented programming when developing a software and consider security risks and ways to mitigate them. Using appropriate techniques and technologies in the online appointment booking system will lower the risk of cyber-attacks and would keep the system running. As no technology is full proof, it is paramount to keep the system updated and timely look for loopholes.

# References

Samuel (2022) Online Booking System: What Is It And How Does It Work? Available from: https://easypractice.net/what-is-online-booking/ [Accessed 14 November 2022].

Sanjana (2019) Benefits Of An Online Appointment Management System In Healthcare Industry. Available from: https://mocdoc.in/blog/benefits-of-an-online-appointment-management-system-in-healthcare-industry [Accessed 14 November 2022].

Hakim, F. (2022) 5 Reasons Clinics Need Online Appointment Scheduling. Available from: https://blog.wavetec.com/en/why-clinics-need-online-appointment-scheduling/ [Accessed 14 November 2022].

Serena, H. (2022) Healthcare Sector Facing 69% Increase In Cyberattacks. Available from: https://www.businessleader.co.uk/healthcare-sector-facing-69-increase-in-cyberattacks/ [Accessed 14 November 2022].

Edward, K. (2022) Biggest Cyber Threats in Healthcare. Available from: https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare [Accessed 15 November 2022].

CTI (2019) Security Threats In Healthcare System. Available from: https://consoltech.com/blog/security-threats-healthcare-systems/ [Accessed 15 November 2022].

Richard, P. (2022) Web Apps Offer A Way In For Cyberattacks In Healthcare Computer Networks. Available from: https://www.medicaleconomics.com/view/web-apps-offer-a-way-in-for-cyberattacks-in-health-care-computer-networks [Accessed 15 November 2022].

Miro (2021) What Are UML Diagrams, And How Can You Use Them? Available from: https://miro.com/blog/uml-diagram/ [Accessed 15 November 2022].

Creately (2022) UML Diagram Types Guide: Learn About All Types Of UML Diagrams With Examples. Available from: https://creately.com/blog/diagrams/uml-diagram-types-examples/ [Accessed 15 November 2022].

Nataliya, S. (2018) Threat Modelling: 12 Available Methods. Available from: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ [Accessed 20 November 2022].

Mitek (2021) Costs And Benefits Of Authentication. Available from: https://www.miteksystems.com/blog/costs-and-benefits-of-authentication [Accessed 20 November 2022].

Jack, M. (2021) Secure Web Gateways 101: Your Primer To An Isolation-Based Approach To Cybersecurity. Available from: https://www.menlosecurity.com/blog/secure-web-gateway-swg-101-your-primer-to-an-isolation-based-approach-to-cybersecurityA/ [Accessed 20 November 2022].

Vijay, K. (2021) What Is Secure Web Gateway? Definition, Benefits And Best Practices. Available from: https://www.spiceworks.com/it-security/network-security/articles/what-is-secure-web-gateway/ [Accessed 20 November 2022].

101 Domain (2019) Why DNS Firewalls Are Essential For Enterprise Security. Available from: https://blog.101domain.com/business-development/dns-firewalls-enterprise-security [Accessed 20 November 2022].

Mishal, R. (2020) 5 Advantages And Disadvantages Of Firewall| Drawbacks & Benefits Of Firewall. Available from: https://www.hitechwhizz.com/2020/03/5-advantages-and-disadvantages-drawbacks-benefits-of-firewall.html [Accessed 20 November 2022].