A web-based appointment and scheduling management information system (ASMIS)

Queens medical centre

Contents

A web-based appointment and scheduling management information system (ASMIS) 1

Queens medical centre 1

Introduction 3

Objective 3

Problem Context 3

Rationale for digital transformation 3

ASMIS - Improving access to on-time care through digital health 4

ASMIS - Is it enough for patient care and satisfaction? 4

ASMIS - Security Requirements 5

Introduction to features and facilities 5

Significance of system security 5

ASMIS - Security by design 5

Key process of ASMIS 6

ASMIS - Threat Modelling Overview 7

Identifying the system components and its interconnections 7

Identifying assets and access points which an attack could occur 8

Identifying potential threats using STRIDE 9

Threat profile for ASMIS 11

Conclusion 12

Reference List 13

Introduction

Objective

Queens medical centre wants to use innovative information and communication technologies to assist them in providing high value services to their community patients (Zhao et al., 2017; Zhang et al., 2014).

Problem Context

As many other clinicians, Queens medical centre is struggling to cope with a high volume of calls, which increases problems for residents to get access to care on time, and the gap between the supply of resources and the demand for healthcare is widening as respond to the rate of growth of the community population. Limitations in communications can be considered barrier to quality care and an adverse effect on the establishment of a friendly customer relationship (Aburayya et al.,2020).

Rationale for digital transformation

Queens medical centre has identified a web-based appointment and scheduling management information system (ASMIS) to help close the gap of respond to the rate of growth of the community population within the catchment area as an approach for ensuring better patient healthcare.

Motivational factors for abandoning current call-based (manual) appointment scheduling;

- ***Appointments limited by office hours***: as calling hours and visiting hours are limited to a particular duration, flexibility is limited and may lead to loss of potential patients or appointments. Considerably, accessibility and availability are two crucial factors of an efficient primary healthcare (Aburayya et al.,2020).

- ***Lower productivity*****:** due to limited staffing and phone lines, waiting times for appointments or registering can often be prolonged and inflexible. That also signifies a loss of potential appointments and patient inconvenience (Zhao et al., 2017).

- ***Room for error and burden on patients***: high volume of calls may allow limited verbal communication during appointment scheduling, which sometimes leads to close calls prematurely without confirming the details of next actions or leads to mistakes such as wrong appointment date or time or sending a patient to wrong specialist (Stokoe, Sikveland & Symonds, 2016) .

- ***Increased resources & expenses*****:** as the volume of calls increase, to have a proper service more personal and/or additional phone lines might be needed. This means an increase in monthly expenses.

ASMIS - Improving access to on-time care through digital health

Considering the motivations for abandoning current appointment scheduling, Queens medical centre has decided to acquire a web-based appointment and scheduling management information system (ASMIS), which will permit many different advantages.

- ***Better Connectivity and time savings*:** easy access to online appointment scheduling and ability to get a timely appointment unimpacted by the schedulers and phone lines. A self-service of 24/7 access for appointments. (Zhang et al., 2014).

- ***Automatic reminders*:** possibility to develop a plugin that will send advance notifications to patients regards to upcoming appointment.

- ***Speedy and Easier appointment management*:**
    - Allowing patients to have more freedom in selecting appointments suitable to their preferences (Zhao et al., 2017).
    - Timely collection, processing and sharing of patients' clinical information-advancing the quality of patient care (Abomhara, 2015; Alhassan, et al., 2016).
    - Ability to maintain online holiday and non-working days for both medical centre and/or doctors, which assist in displaying availability for each doctor
    - Ability to maintain patients' consultation history, medical reports, which also has other benefits such as reduction in paper use and duplication of testing (Afrin & Arifuzzaman, 2020).
    - Provide more visibility for the medical centre, allowing flexibility for handling/managing upcoming appointments as well as better control over doctors' schedule and employee productivity.

- ***Monetary Savings*:**
    - Reduce the burden of hiring additional staff or having additional phone lines to meet to increase demand.

ASMIS - Is it enough for patient care and satisfaction?

Paddison, et al. (2013) through their research in primary care in England, emphasised that helpfulness of receptionists as a prominent characteristic of patients' experience in health care

In early studies regard to patient priorities within primary health care, "humaneness" as a means of improving the sensitivity for patients' needs, proved to be important (Wensing et al., 1998). Compared to online appointment scheduling, verbal communications allow maximum flexibility in complex circumstances as it tempt to deliver experiences such as "treats you like an individual", "sensitive to feelings" and "understanding".

Another important to consider is the impact of the socio-demographics on the choice of using a web-based appointment service (Zhang et al., 2014) as patients' decision to accept

or reject a web-based appointment service is influenced by patient's prior experience of using the Internet, computer literacy, prior awareness of e-health applications, access to the Internet (Wensing et al., 1998) or just personality differences informed by their experiences and personal dispositions (Shen et al.,2019).

Considering the above communication-related factors and underling the need to balance the demand for appointments with the centre capacity, a hybrid scheduling strategy that incorporates walk-ins, call-in and online appointment scheduling allows the optimal path to lower the patient waiting period as well as the reception to exit cycle-time. Aburayya et al. (2020) proposed a similar approach as a means of solving efficiency issues related to performance optimisation, flexibility and patient satisfaction.

ASMIS - Security Requirements

Introduction to features and facilities

Considering the main requirements for the proposed ASMIS, there are three sets of functionalities for a web-based appointment and scheduling management.

- Online registration – new user registration, log-in, patient profile creation, selection of date and physician
- Data management – view, add, delete, modify appointment and patient data. Maintain doctors' profiles.
- Health records management - data backup and restore.

Significance of system security

However, with the increasing amount of personal information and patient data being collected, the more valuable and sensitive information become (Abomhara, 2015; Gerdes & Fensli, 2015). Exposing confidential health information accidentally or deliberately must be prevented by the Queens medical centre or information technology service providers, as this may lead to stern legal punishments for violating privacy laws such as General Data Protection Regulation (GDPR) by the European Commission (2012).

Therefore, patient information requires to be shared securely in a manner that guarantees privacy (Haque & Pranto, 2020; Alhassan, et al., 2016) and ASMIS should have a 'security by design', to be vigilant and careful with protecting both the information and those providing the information.

ASMIS - Security by design

Inability to account for all possible threats against ASMIS at the development leads to insufficient security, allowing ASMIS to be vulnerable to security breaches (Abomhara, 2015).

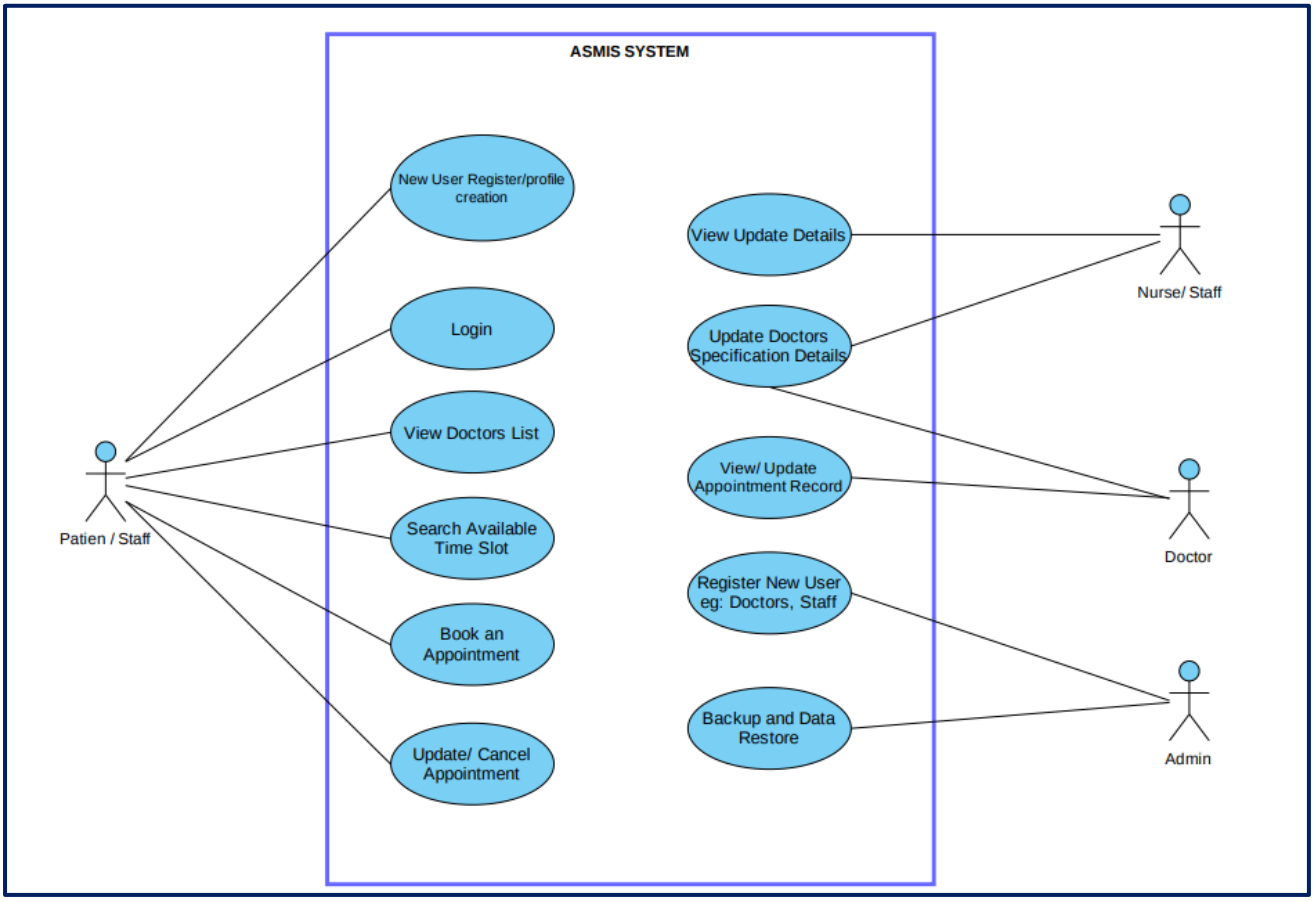
Therefore, by understanding processes; system components; system complexity; identifying all possible threats and rating them based on their probability and impact, final decision need to be taken, either to mitigating threats or accept the associated risks (Alhassan, et al., 2016; Shostack, A.,2014).

Key process of ASMIS

Through ASMIS user/patient can select a doctor and book an appointment. Prior to the booking, the patient must register into the ASMIS through Queens medical centre webpage. On the other hand, Queens medical centre receptionist can login and create a patient profile or access existing patient profile to book an appointment for walk-in/call-in patients. Thereafter, Queens medical centre healthcare professionals (i.e. receptionist, doctors) can either accept or reject the appointment and an acknowledgement is sent to the patient through the email, which was entered at the account registration.

As the patient visits the doctor with whom the appointment has been made, the doctor enters the patient health notes and treatment history into the system through doctor's account login. Both the patient and the Queens medical centre healthcare professionals have different access rights to information in the databases. Patient is allowed to access his/her medical history, while the healthcare professionals (i.e. doctors, nurses) keeps own patient records that can be used during treatment process. ASMIS updates its historical database through daily backups.

Figure 1 - Use case diagram



ASMIS - Threat Modelling Overview

As personal medical data are privacy-critical, there are several security measures to be taken into consideration when gathering, communicating and accessing information (Gerdes & Fensli, 2015) via ASMIS infrastructure.

On the process of threat modelling, extensive research have been undertaken on Open Web Application Security Project (OWASP) (Hong, et al., 2019), Microsoft STRIDE model (Abomhara et al., 2015), Microsoft's development of the security life cycle (SDL) (Yuan et al., 2015) and the Process for Attack Simulation and Threat Modeling (PASTA) (Ucedavélez & Morana, 2015).

However, in the ASMIS threat modelling, STRIDE is it helps to describe all potential attacks while mapping of information security requirements(Pendergrass, et al., 2013; Yuan et al., 2015).

Here, threat modelling process is divided into the four main phases,

- Identifying the system components and interconnections,
- Identifying assets and access points which an attack could occur,
- Identifying potential threats using STRIDE
- Building a mitigation plan based on proposed countermeasures.

Identifying the system components and its interconnections

Figure 2 - Architecture overview of ASMIS

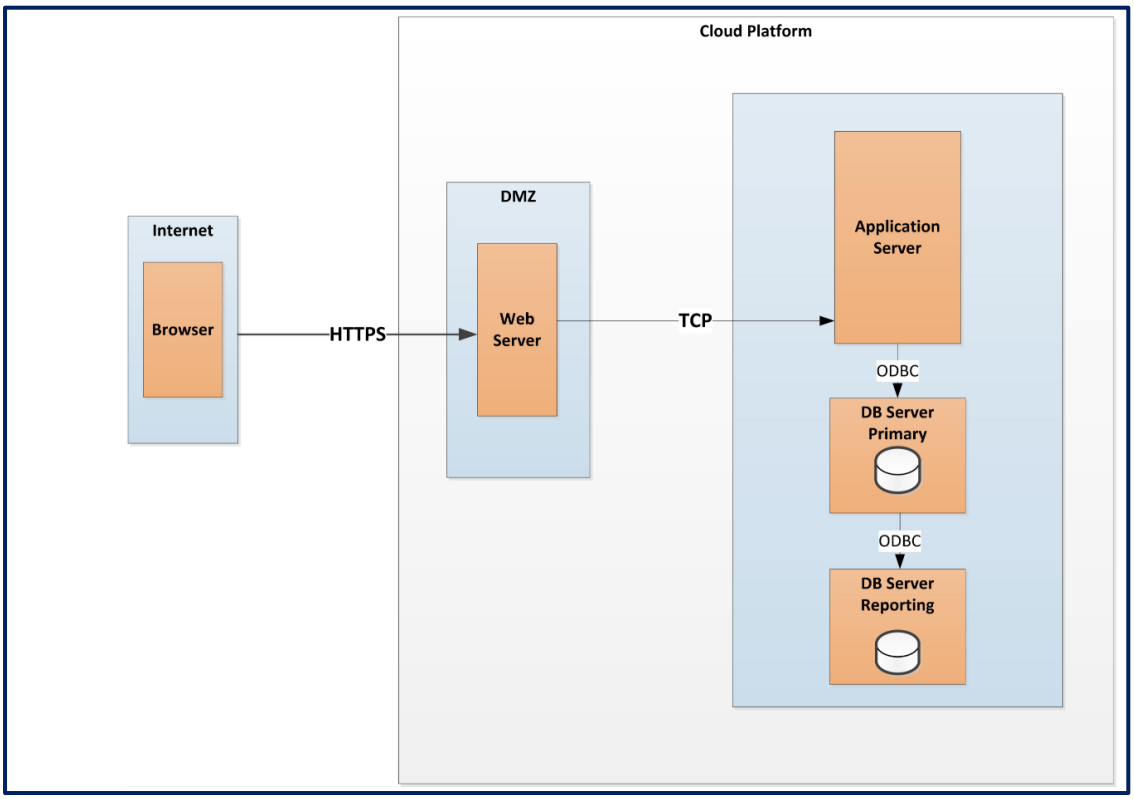
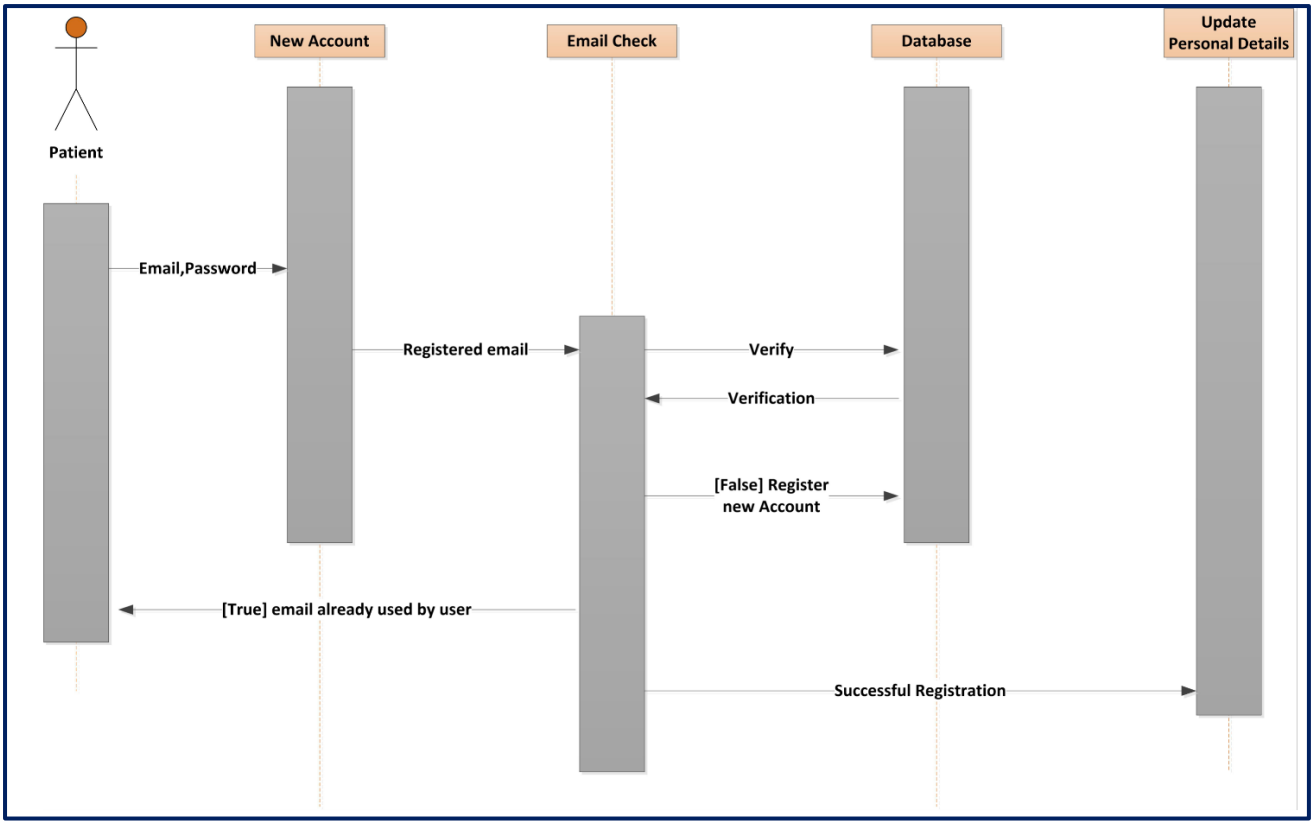


Figure 3 - Sequence diagram for new account registration (patient)



Identifying assets and access points which an attack could occur

An **asset** is anything that has business/operational value. Assets identification is focal for threat modelling as they are essentially threat targets (Gerdes & Fensli, 2015), which attackers are keen to gain access either to control or destroy.

Value of the assets to the operation/business can be define based on their vulnerabilities regards to integrity, confidentiality and accessibility (CIA) (Stewart et al., 2015: 4-13).

Examples in ASMIS:

- All patient-related data
- Healthcare service members' (i.e. doctors, receptionist, other medical assistance) login credentials to log into the system.
- Login credentials used by a patient
- System configurations
- System Event logs

Exposure points through which potential attackers can manipulate system to gain privileged access to assets are regarded as **access points**. Therefore, it is crucial to defined trust levels, which identify levels of trust boundaries to access components within the system (Gerdes & Fensli, 2015).

Examples of trust levels for threat agents

- Patient - access to his/her own personal medical records and communications maintained with the medical centre.
- Doctors & Nurses - have access only to the medical records and information of patients they are responsible for.
- Personal Assistants (i.e. receptionists) - have access to basic patient's registration data and appointment information.
- System Administrator – access to all system components but not health-related records of the patients.

Identifying potential threats using STRIDE

Threats may come in the form of insider (authorized) or outsider (unauthorized) access.

Classification of threats in to six classes following the Microsoft STRIDE model (Yahya, Walters & Wills, 2015)

- Spoofing – using false identity to gain entree into unauthorised assets.
- Tampering – unauthorized modification of data to mount an attack.
- Repudiation – ability denying performing an action, which cannot be proved otherwise.
- Information disclosure – unwanted disclosure of private data to an authorised user.
- Denial of service – unavailability of access to resources for valid users.
- Elevation of privilege – an unprivileged user gains privileged access to an asset.

ISO/IEC 27002 (Based) list summary of requirements in information security, which was also reassessed and summaries by Yahya, Walters & Wills (2015) in their extensive analysis on key aspects of best practices required/proposed by some of the prominent global security organisations.

'Information security: Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved' (ISO/IEC 27002, 2018)

Summary of organisational requirements based on the study carried out by Yahya, Walters & Wills (2015)

Table 2. Summary of security requirements from organisations

Organisation / Requirement	CSA (2013) [15]	NIST (2013) [17]	ENISA (2009) [19]	CPNI (2014) [21]	ASD (2014) [24]
Confidentiality	√	√	√	√	√
Integrity	√	√	√	√	√
Availability	√	√	√	√	√
Non-repudiation	√				
Authenticity	√		√	√	√
Reliability			√	√	√

(Yahya, Walters & Wills, 2015:553)

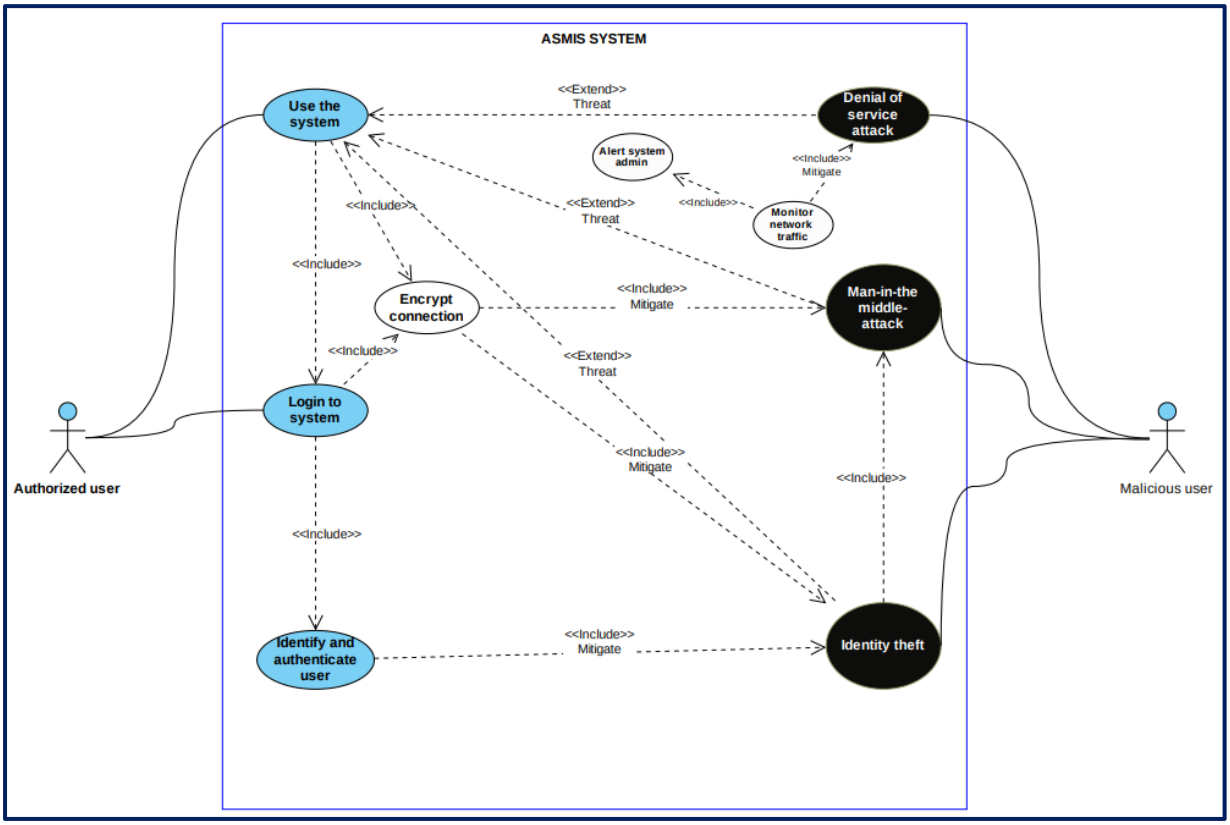
Organisation names by abbreviations (reference to above Table 2 - Yahya, Walters & Wills, 2015)

- ENISA - European Network and Information Security Agency
- NIST - The National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organisations
- CPNI - The United Kingdom Centre for the Protection of National Infrastructure
- ASD - Australian Signals Directorate
- CSA - Cloud Security Alliance

Threat profile for ASMIS

Misuse case diagram - an example of threat identification and mitigation plan based on scenarios that can bring harm to the ASMIS. Mitigation mechanism is identified based on the risk assessment performed underlining priority assumptions.

Figure 4 - Misuse case diagram (Skramstad, T. et al.,2020)



STRIDE was used in the ASMIS threat identification process as it helps to describe all potential attacks while mapping of information security requirements. The mapping of threat to security requirements is crucial as it helps to reflect the impact of each threat to the security objectives, which ASMIS is planning to achieve as a reliable system. Mitigation controls are identified based on risk assessment of threats.

Security Requirements	Threat	STRIDE	Mitigation Controls
Authenticity Confidentiality	Identity loss or identity sharing (Abomhara et al., 2015) i. Patients revealing login credentials to someone ii. Patient or healthcare professionals /or system admins mistakenly revealing their login credentials publicly.	Spoofing Identity Elevation of Privilege Information disclosure	Packet Filtering Use of encryption methods Zero-Trust Approach
Authenticity Integrity Confidentiality Availability	Account/Service Hijacking (identity theft) i. Account hijacking (Hong et al. 2018) from SQL injection or privilege escalation (CSA, 2013).	Elevation of privilege Spoofing Identity Information disclosure Tampering	Use of encryption methods (proactive measures)
Integrity Non - Repudiation	Data tampering i. Patient or healthcare professionals intentionally or unintentionally modify, add and/or delete data due to inapplicable accesses (Abomhara et al., 2015).	Tampering Repudiation	Auditing/review of access privileges (proactive measures)
Availability	Distributed denial-of-service (DDoS) i. A malicious attempt to disrupt normal traffic of a targeted server with a flood of Internet traffic (Hong et al. 2018) and result in denial-of-service condition.	Denial of service	Monitor network traffic (proactive measures) and alert System Admin (reactive measures)
Authenticity Integrity Confidentiality	Man-in-the-Middle Attack i. Attacker is placed between the sender and the receiver, who can, not only spoofs IP (Internet Provider) packets to hijack a connection to the server and modify data in order to mislead the receiver (Xin & Xiaofang, 2014).	Spoofing Identity Tampering Information disclosure	Use of encryption methods (proactive measures)

Conclusion

The study discusses potential benefits of adapting ASMIS as a hybrid approaches for appointment scheduling at the Queen Medical Centre. As a threat modelling techniques STRIDE was used as it helps to assess the identified threats more closely while mapping them with security objectives of the ASMIS.

One of the key security controls that needs to be in place in order to mitigate authenticity, integrity and confidentiality related vulnerabilities in ASMIS, is to adapt encryption methods to safeguard access privileges. The nature of ASMIS requires maintenance of high level of confidentially of patient data. Therefore, structured security testing methodology needs to be in place to review access on regular basis as a proactive measure.

Reference List

Abomhara, M., Køien, G. & Gerdes, M. (2015) A STRIDE-Based Threat Model for Telehealth Systems. Available from: https://www.researchgate.net/publication/291766457_A_STRIDE-Based_Threat_Model_for_Telehealth_Systems [Accessed 21 November 2020].

Aburayya, A., Al-Marzouqi, A., Al Ayadeh, I., Albqaeen4, A. & Mubarak, S. (2020) Evolving a Hybrid Appointment System for Patient Scheduling in Primary Healthcare Centres in Dubai: Perceptions of Patients and Healthcare Provider. Available from: https://www.researchtrend.net/ijet/pdf/Evolving%20a%20Hybrid%20Appointment%20System%20for%20Patient%20Scheduling%20in%20Primary%20Healthcare%20Centres%20in%20Dubai%20Perceptions%20of%20Patients%20and%20Healthcare%20Provider%201768MBAA.pdf [Accessed 18 November 2020].

Afrin, A. & Arifuzzaman, A. (2020) e-Health in Developing Countries: Bangladeshi Perspective. *International Journal of Engineering and Advanced Technology*. 9(3): 908-914. DOI: 10.35940/ijeat.A1837.029320.e

Alhassan, J., Abba, E., Olaniyi, O. & Waziri, V. (2016). Threat Modelling of Electronic Health Systems and Mitigating Countermeasures. Available from: https://www.researchgate.net/publication/311238739_Threat_Modeling_of_Electronic_Health_Systems_and_Mitigating_Countermeasures [Accessed 19 November 2020].

Anjum, F. et al. (2018) 'Online health care', *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual, 580–583. DOI: 10.1109/CCWC.2018.8301617.

Collmann, J. & Cooper, T. (2007) Breaching the security of the Kaiser Permanente internet patient portal: the organizational foundations of information security, *Journal of the American Medical Informatics Association*, 14(2): 239–243.

Cloud Security Alliance (CSA). (2013) *The Notorious Nine: Cloud Computing Top Threats in 2013 Report*. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf [Accessed 22 November 2020].

European Commission. (2012) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Available

from: https://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF [Accessed 27 September 2020].

Gerdes, M. & Fensli, R. (2015). *End-to-end Security and Privacy Protection for Co-operative Access to Health and Care Data in a Telehealth Trial System for Remote Supervision of COPD-Patients*. Available from: https://ep.liu.se/ecp/115/005/ecp15115005.pdf [Accessed 22 November 2020].

Haque, A. & Pranto, T. (2020) Health Data Security: A Privacy-Preserving Proposed Strategy for Bangladesh. *International Journal of Emerging Technologies in Engineering Research (IJETER)*. Available from: https://www.researchgate.net/publication/342697605_Health_Data_Security_A_Privacy-Preserving_Proposed_Strategy_for_Bangladesh [Accessed 20 November 2020].

Hong, J., Nhlabatsi, A., Kim, D., Hussein, A., Fetais, N. & Khan, K. (2018). Systematic Identification of Threats in the Cloud: A Survey. *Computer Networks*. Available from: https://www.sciencedirect.com/science/article/pii/S1389128618308259 [Accessed 21 November 2020].

ISO/IEC 27000. (2018) Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 21 November 2020].

Otte-Trojel, T., Bont, A., Rundall, T. & Van de Klundert, J. (2015). What do we know about developing patient portals? A systematic literature review. *Journal of the American Medical Informatics Association*. Available from: https://www.researchgate.net/publication/281514712_What_do_we_know_about_developing_patient_portals_A_systematic_literature_review [Accessed 19 November 2020].

Paddison, C. et al. (2013*) Drivers of overall satisfaction with primary care: evidence from the English General Practice Patient Survey*. Available from: https://onlinelibrary.wiley.com/doi/full/10.1111/hex.12081 [Accessed 18 November 2020].

Parekh, M. & Saleena, B. (2015) Designing a Cloud Based Framework for HealthCare System and Applying Clustering Techniques for Region Wise Diagnosis. *Procedia Computer Science*. 50: 537-542. DOI: 10.1016/j.procs.2015.04.029.

Pendergrass, J., Heart, K., Ranganathan, C., & Venkatakrishnan, V. (2013) 'A Threat Table Based Approach to Telemedicine Security', *Transactions of the International Conference on Health Information Technology Advancement*. Available from: https://core.ac.uk/download/pdf/144155387.pdf [Accessed 20 November 2020].

Ray, S. & Biswas, G. (2012) *Design of RSA-CA Based E-Health System for Supporting HIPAA Privacy-Security Regulations*, Procedia Technology, 6: 954–961.

Ryan, K. (2011) *DIY appointments for patients*, Medical Journal of Australia, 195(7): C6–C7. Available from: http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=edo&AN=66938125&site=eds-live [Accessed 19 November 2020].

Schoenfelder, J., Bretthauer, K., Wright, P. & Coe, E. (2019) Nurse Scheduling with Quick-Response Methods: Improving Hospital Performance, Nurse Workload, and Patient Experience. *European Journal of Operational Research*. 283: 1. DOI: 10.1016/j.ejor.2019.10.047.

Shen, N. et al. (2019) Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics*. 125: 1-12. DOI: 10.1016/j.ijmedinf.2019.01.014.

Shostack, A. (2014) *Threat Modeling: Designing for Security*. Indiana: John Wiley & Sons, Inc. Available from: https://moodle.ufsc.br/pluginfile.php/2377555/mod_resource/content/2/Threat%20Modeling.pdf [Accessed 21 November 2020].

Skramstad, T. et al. (2020). *Security Testing of Web Based Applications*. Available from: https://www.researchgate.net/publication/268418932_Security_Testing_of_Web_Based_Applications [Accessed 21 November 2020].

Stewart, J.M., Chapple, M. & Gibson, D. (2015) CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. 7th ed. Wiley India Pvt. Ltd.

Stokoe, E., Sikveland, R. & Symonds, J. (2016*) Calling the GP surgery: patient burden, patient satisfaction, and implications for training*. Available from: https://bjgp.org/content/66/652/e779#ref-1 [Accessed 18 November 2020].

Ucedavélez, T. & Morana, M. (2015) *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. New Jersey: John Wiley & Sons, Inc.

Vermeir, P. et al. (2015*) Communication in healthcare: a narrative review of the literature and practical recommendations*. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4758389/ [Accessed 18 November 2020].

Wensing, M., Jung, H., Mainz, J. & Olesen, F. (1998*) A systematic review of the literature on patient priorities for general practice care*. Available from: https://www.sciencedirect.com/science/article/pii/S0277953698002226 [Accessed 18 November 2020].

Xin, T. & Xiaofang, B. (2014) *Online Banking Security Analysis based on STRIDE Threat Model*. Available from: http://article.nadiapub.com/IJSIA/vol8_no2/28.pdf [Accessed 18 November 2020].

Yahya, F., Walters R. & Wills, G. (2015) Modelling Threats with Security Requirements in Cloud Storage. *International Journal for Information Security Research*. 5: 551-558. DOI: 10.20533/ijisr.2042.4639.2015.0063.

Yuan, X., Nuakoh, E., Williams, I. & Yu, H. (2015). Developing Abuse Cases Based on Threat Modeling and Attack Patterns*. Journal of Software*. 10 (4): 491-498. DOI: 10.17706/jsw.10.4.491-498.

Zhang, H., Zhang, H., Wang, X., Yang, Z. & Zhao, Y. (2017) Analysis of Requirements for Developing an mHealth-Based Health Management Platform. *JMIR mHealth and uHealth*. 5(8): e117. DOI: 10.2196/mhealth.5890

Zhang, X., Yu, P. & Yan, J. (2014*) Patients' adoption of the e-appointment scheduling service: A case study in primary healthcare*. Available from: https://www.researchgate.net/publication/264463423_Patients'_adoption_of_the_e appointment_scheduling_service_A_case_study_in_primary_healthcare [Accessed 17 November 2020].

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B. & Simoes, E. (2017) Web-Based Medical Appointment Systems: A Systematic Review. *Journal of Medical Internet Research*. 19(4): e134. DOI: 10.2196/jmir.6747