Web-Based Appointment and Scheduling Management Information System (ASMIS)

Report

Word Count: 1931

1. Introduction

Queens medical center caters for all unwell residents within its catchment area and the receptionist has been experiencing a high volume of calls by prospective patients. The prospective patients are required to telephone the community clinic for an appointment to schedule a consultation with one of the clinic's specialists. Due to the high volume of calls, the clinic's management has chosen to implement a web-based appointment and scheduling management system (ASMIS) which will allow online prospective patients to submit vital information to determine which specialist would be best suited for the patient.

According to Zhao et al (2017) who carried out research on 21 Web-based appointment and scheduling systems, the benefits of adopting a ASMIS had been a reduction in no-show appointments, decrease in waiting times, reduction in staff labor and an improvement in satisfaction.

This web-based system has many benefits to improve the operation of Queens medical center and patient services, however, due to the design of the web-application to be implemented, it will arrive with privacy and security challenges which will need to be accessed, implemented within the rules, regulations and compliance of user privacy and safety.

This report will observe Use case and Abuse case, cyber threats and mitigations, the systems architecture, privacy regulations and risk frameworks to strengthen the security of the system, safety of the patients and enforce Confidentiality, Integrity and availability of data.

2. Statement

2.1 What:

Confidentiality of the Patients data needs to be protected and compliance achieved with national and international privacy and data protection laws.

Integrity of the Patients data also needs to be ensured to allow the correct diagnosis, treatment and safety of the patient.

Availability of the services needs to be maintained for the safety of the patients and to ensure that all those who require medical attention can receive it in a timely manner.

2.2 Why:

Conforming to the security CIA triad provides a solid foundation and guidance for further policy frameworks to be implemented which will increase the security of the system, infrastructure, architecture, staff and patients.

2.3 How:

By following the recommended Unified Modeling Language diagrams, threat modeling techniques, risk assessments and object oriented design framework that includes security system implementation approaches, this will enable a more secure and compliant system to be developed.

As the software will be acquired, we will seek to focus our efforts on the “security required aspect” over the “functional aspect”. Although the security requirement approach can restrict or constrain the applications functionality (UoE, 2022), the benefits of this approach prepares the system for chaotic users, malicious activities and adversarial behavior.

3. Unified Modeling Language Diagrams

Unified Modeling Language (UML) diagrams allow teams to specify, visualize, and document the model of the software systems, its structure and design (OMG, 2022) while providing us with the ability to create an understandable schematic for the proposed behavior, structure and interaction of our system.

3.1 UML Use Case

The Use case diagram illustrates the behavioral sequence of actions and executions that the system will perform and highlights the functional requirements between the actors and system (Figure 1). This Use case diagram provides a visual schematic to identifying where documentation and risk assessments need to be considered and should be combined with the Abuse case diagram (Figure 2) to observe the function, threats and impact within the proposed ASMIS.

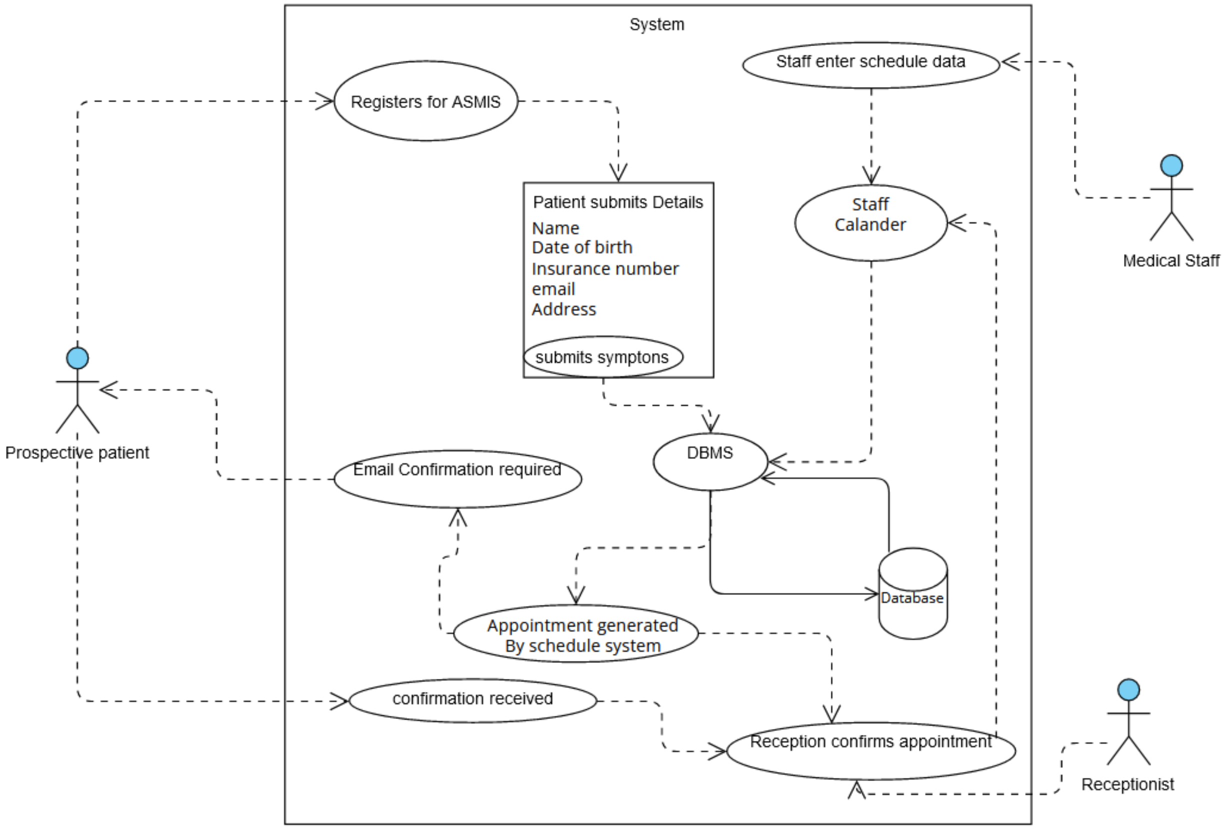


Figure 1: Use Case

3.2 UML Abuse Case

The Web-based Appointment and Scheduling Management Information System (ASMIS) will provide various attack vectors for adversaries to explore. Due to the threats posed by having a web-based application, we have implemented an “Abuse case diagram” (Figure 2) to identify the possible attack vectors and security vulnerabilities via the actors (users), software and hardware. This allows us to discover the impacts and to implement specific and defined Threat Modeling Techniques. Combining the Abuse case with the Use Case will give a clearer understanding of the system layout, users and possible vulnerabilities.

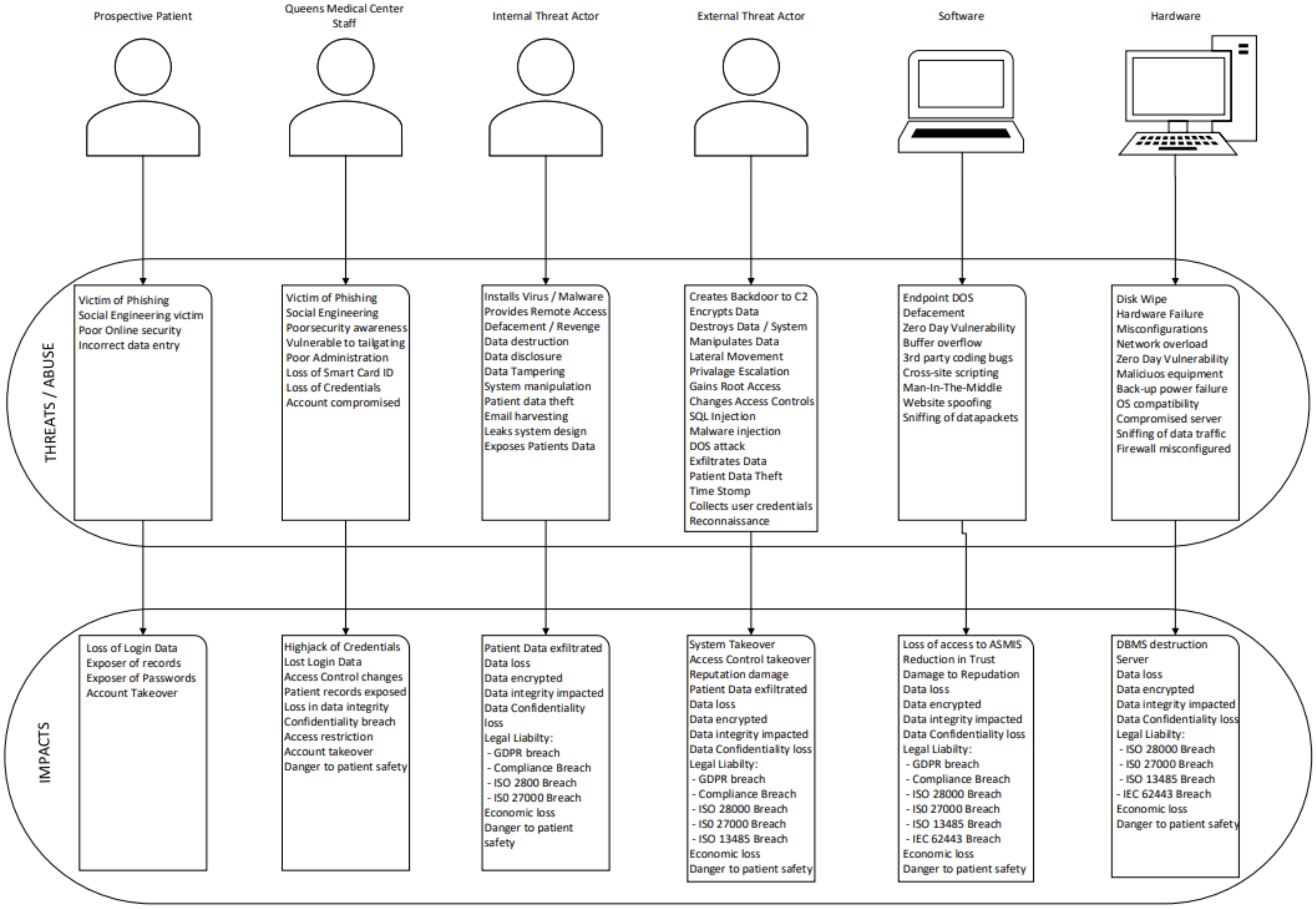


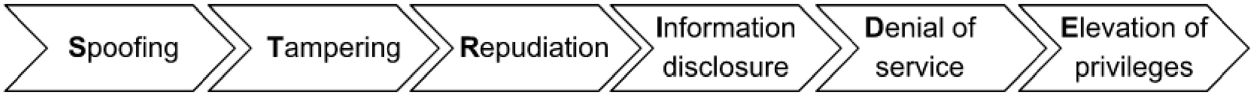
Figure 2: Abuse Case

4. Threat Modeling Techniques

For the integration of the ASMIS to be accepted by the prospective patients, their privacy and data should be a priority and to remain compliant with GDPR. Due to this, it is recommended that we implement two separate threat methodologies. STRIDE methodology for the system architecture and the Lockheed Martin Cyber Kill Chain methodology.

4.1 STRIDE

This threat modeling technique will aid in identifying threats and help suggest which mitigating technique is most relevant, especially if microsoft products will be used.



Spoofing

The identity of the patient/staff can be spoofed during login.

Mitigate with user multi-level authentication.

Tampering

Threat actors could tamper with data internally via lateral movement and escalation of privileges.

Mitigate with MAC address ID, TLS, zero-trust, two-step authentication and logging.

Repudiation

Threat actors could add and alter keys via the repository database.

Mitigate by logging the key hash at time of creation on a separate system via a unidirectional gateway with alternative trust levels to the database.

Information disclosure

Threat actors may discover patient data being sent through the system during patients record updating.

Mitigate by IPsec and/or TLS encryption.

Denial of service

Threat actors could overload the appointment system by directing thousands of appointment requests simultaneously and cause the site to crash.

Mitigate by implementing flow-rate limitation

Elevation of privileges

Threat actors may move laterally through the system to discover higher level privileges and via initial phishing exercises.

Mitigate by hardening databases and systems. Apply MAC address ID, TLS, zero-trust, two-step authentication and logging.

4.2 Lockheed Martin Cyber Kill chain

This threat model framework helps to identify, protect and mitigate against adversaries at all stages of their attack by providing five mitigation approaches to the seven phases of the attack, see table 1: Course of Action Matrix.

Table 1 illustrates that depending on which stage an attacker is at, we can either detect, deny, disrupt, degrade or deceive by using various tools, hardware and software. Two examples of using the course of action matrix would be that we could deny the attacker carrying out reconnaissance by ensuring that we have a Firewall with Access Control Lists implemented. The second example is that we could degrade the attackers attempt at stage 6 (C2 - command and control) by using Tarpit which is a service on a computer or server that purposely delays an incoming connection.

Key:

NIDS = Network Intrusion Detection system

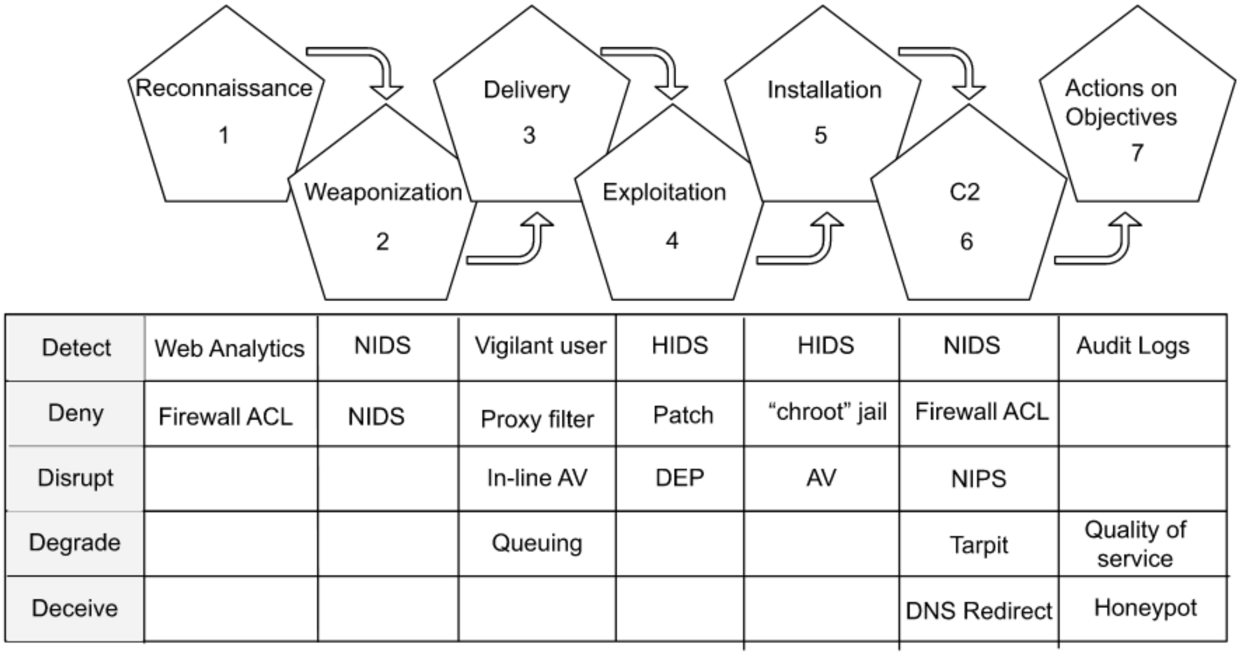
HIDS = Host Intrusion Detection System

DEP = Data Execution Prevention

ACL = Firewall Access Control Lists

AV = Antivirus

C2 = Command and control



Detect	Web Analytics	NIDS	Vigilant user	HIDS	HIDS	NIDS	Audit Logs
Deny	Firewall ACL	NIDS	Proxy filter	Patch	“chroot” jail	Firewall ACL	
Disrupt			In-line AV	DEP	AV	NIPS	
Degrade			Queuing			Tarpit	Quality of service
Deceive						DNS Redirect	Honeypot

Table 1: Course of Action Matrix

4.3 Risk Assessment framework - NIST Privacy Framework

Taking the UML diagrams and threat modeling into consideration, we could then consider implementing the NIST Privacy Frameworks five functions to help manage risk associated with privacy (NIST, 2020).

Five functions are:

1. Identify-P. *Identify privacy risks for users*
2. Govern-P. *Implement privacy governance structure.*
3. Control-P. *Enable individuals to manage data safely.*
4. Communicate-P. *Ensure data privacy is understood by all*.
5. Protect-P. *Implement data processing safeguards*.

5. Secured object-oriented design

5.1 Authentication for authorisation-

Specialist doctors could be assigned a Medium Access Control (MAC) address and biometric authentication. These two forms of authentication must be used together in order to gain access to patients data and for making data modifications. This ensures data confidentiality and integrity as only pre-designated devices on the network have access. These processes still require logging and monitoring due to the potential of a MAC address spoofing attack.

5.2 Software Bill of Rights (SBOM)

Ensure that the chosen application has SBOM documentation. This will allow us to understand how the software and hardware was created, what was used in the development process and how we can harden the system against current and future vulnerabilities.

5.3 Database and Database management system (DBMS) Security

It is paramount that the confidentiality, integrity and availability of the Data provided by the patient and specialists is maintained by securing the Database and DBMS.

Securing the DBMS systems and all the associated applications can be achieved by implementing the following recommendations.

5.4 Secure configuration

- □ Configure and enable Database Management System (DBMS) security controls while also ensuring that the database services run under a low privilege account setting.
- □ Enforce regular patches and security updates.
- □ Remove and change all default accounts.
- □ Logs should be stored on a separate system.
- □ Ensure that the backups are encrypted

5.5 Secure authentication

- □ Ensure all access to the database is authenticated
- □ Authentication and monitoring should be required to access the database.
- □ Use strong passwords
- □ Do not store database credentials in source code repositories or application source code and always encrypt.
- □ Consider storing encrypted credentials outside of webroot and in a configuration file with user permission settings.

- □ To mitigate against privilege escalation vulnerabilities, ensure that the database owner is not the account owner.

5.6 Secure communication

Reduce the ability of adversaires being able to connect to the backend database by isolating it as much as possible by following these recommendations:

- □ Force access over a named pipe or local socket and disable TCP.
- □ Separate the application server from the database server via separate DMZ architecture.
- □ Configure firewalls to restrict access to certain ports
- □ Ensure the database is configured to only allow encrypted connections.
- □ Use trusted certificates.
- □ Use TLS and digital certificates.

6. Data Protection and Privacy

Ensure that the data protection tools include

- □ Encryption and Tokenization capabilities
- □ Data security optimisation capabilities
- □ Risk analysis capabilities
- □ Data activity monitoring
- □ Data insights discovery

6.1 Policy Frameworks

Elements of the following ISO policies can be selected, implemented and audited to ensure that the software and hardware assets are secured while informing and training the human actors on good cyber-hygiene, privacy and procedures (OSI, 2020).

- □ ISO 27000 series of standards is a policy framework specifically for information security matters.
- □ ISO 27799 is specialized towards health informatics and implemented via ISO 27002 for patient privacy.
- □ ISO 31000 is to be applied within existing management systems to formalize and improve risk management processes

6.2 Regulation

General Data Protection Regulation (GDPR) needs to be strictly adhered to and consistently analyzed.

According to GDPR (2022), Personal data may not be processed unless there is at least one legal basis to do so

- □ **Article 6** states the lawful purposes are:
    - □ (a) If the data subject has given consent to the processing of his or her personal data;
- □ **Article 37** requires appointment of a Data Protection Officer if processing is carried out by a public authority.

7. Considerations

7.1 Data protection tools

It is highly recommended that we have a logging data protection system in the tool while also having at least four of the following abilities.

- □ **Discovery** functionalities to be able to provide insights into the data.
- □ **Data activity monitoring** is useful in detecting abnormal activities.
- □ The tool must have **encryption** and **tokenisation** capabilities.
- □ The tool must have **data security optimisation** and **risk analysis** capabilities.

Recommendations (Tools)

- □ ElasticSearch Stack with logging abilities (Security Information and Event Management)
- □ Microsoft defender for endpoints if we standardized with MS products
- □ Malcolm for PCAP Network traffic analysis
- □ SOAR (security orchestration, automation and response)

7.2 (C5) Cloud Computing Compliance Controls Catalog is a minimum standard in cloud security if the decision is made to move data to Cloud Service Provider (BSi, 2020)

8. Conclusion

Although previous studies have highlighted the positive benefits of having an ASMIS implemented, we have to remember that it is a technology which may still be too advanced for the elderly and vulnerable patients, therefore, I recommend that we also consider a secondary option to allow for those individuals to make an appointment. Staff should also be mandated to attend in-house security and privacy training.

References

BSi. (2020) Orientation guide to documentation of compliance according to Section 8a (3) BSIG. *Bundesamt für Sicherheit in der Informationstechnik*. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/oh_nachweise_en.pdf?__blob=publicationFile&v=6 [Accessed on 11 August 2022]

GDPR. (2022) Complete guide to GDPR compliance. Available from: https://gdpr.eu/ [Accessed on 13 August 2022]

ISO. (2022) *Standards: International Organization for Standardization*. Available from: https://www.iso.org/home.html [Accessed on 11 August 2022]

NIST. (2020) *NIST Privacy Framework: A tool for improving privacy through enterprise risk management*. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf [Accessed on 11 August 2022]

OMG. (2022) Unified Modeling Language. Available from: https://www.uml.org/what-is-uml.htm [Accessed on 06 August 2022]

UoE. (2022) *Approaches to security design - Software requirement Lecturecast 3* [Lecturecast] LCYS_PCOM7E June 2022 Launching into Cyber Security 2022. University of Essex Online

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)*:* 6747 Available from: https://www.jmir.org/2017/4/e134/ [Accessed on 08 August 2022]