The Queens medical centre requires an automated booking system for prospective patients to book specialist treatment. To book treatment will involve making an initial determination of the necessary specialist and their availability for the consultation. The Queen's medical centre management has decided on using a web-based Appointment and Scheduling Management Information System (ASMIS), which is being installed by the medical centre IT team.

This report will identify the potential cyber threats to the users of ASMIS and how these threats can be mitigated. It will also examine the ASMIS system's benefits as a web-based platform and identify potential threats. This report will utilise the Unified Modelling Language (UML) to illustrate a Use Case, an Abuse Case, a Class diagram and finally, a Behavioural Sequence diagram. These diagrams will show how threat modelling techniques can be used to highlight potential cyber threats and mitigate them. To support the UML diagrams, this report will discuss UML modelling techniques and why these particular diagrams have been used. Finally, this report will explore the Cyber Security technologies and their strengths and weaknesses that will be used to evaluate the security of the ASMIS platform.

UML is a method of graphically depicting the artefacts of a software system. The UML provides standardisation for writing system blueprints from conceptual to the physical, from database schemas to software languages. UML was born out of a need to deal with a growth in object-orientated programming during the 1970s to the 1980s, growing to over fifty by 1994. Three leading proponents emerged during the 1990's Booch, Jacobson and Rumbaugh. They began to adopt elements from each other's methods and then decided to unify their ideas into a single 'Unified Modeling Language'. Three goals were established as they began the unification. These were to model a system from concept to deliverable element, tackle complexity, scale and criticality of systems, and create a modelling ethos that humans and artificial intelligence could use. UML 1.1 officially released in 1997 after ratification by the Object Management Group (OMG) (Booch et al., 1999).

This report will utilise UML diagrams and modelling techniques to explore the potential cyber security threats to the ASMIS system. The UML will be used to depict the ASMIS systems and the cyber threats graphically. Threat modelling (TM) will be used to identify potential cyber threats to the ASMIS system within the UML diagrams. Several threat models can be used. This report will make use of STRIDE, Abuse case, Class diagrams and Behavioural Sequence diagrams.

STRIDE is a pneumonic and was first introduced by Microsoft in 1999 for their developers to explore threats to their products. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Escalation of Privileges. Using the STRIDE methodology allows security personnel to brainstorm potential threats using whichever of the six classifications is relevant to the system (Microsoft 2019). The Abuse case can be seen as a way of showing how an existing user of a system can take advantage of any weakness inherent in the system or take advantage of an unexpected feature of the system (OWASP 2021b). Class diagrams have been used for object-orientated modelling and detailed modelling that can be used for programming code. In this report, they will be used for data modelling of the ASMIS system and then, in collaboration with the Behavioural Sequence diagram, will highlight the security threats and how they may be mitigated.

To establish a threat profile, we must first understand the critical vulnerabilities an attacker will use. OWASP ( Open Web Application Security Project) is an organisation working on a non-profit basis to improve software security. OSWASP has identified ten web application security risks (OSWASP 2021a). To combat these ten most common vulnerabilities, specific tools can be utilised. Threat modelling has been discussed above, and these will be covered in more detail further in the report. However, there is a tool that can also be used to evaluate the potential threat of a vulnerability to the ASMIS system, and that is CIA, an acronym that stands for Confidentiality, Integrity and Availability. Each of these principles forms part of the CIA Triad (Walkowski 2019). Confidentiality is how Queens medical centre will keep its data secure and control access to it. Integrity is how Queens medical centre will ensure none of that data has been tampered with. Finally, Availability ensures that only authorised users with the correct level of authority can access the data at any given time. Therefore the data is safe, reliable and authentic and only accessed by authorised individuals (Yin 2020).

Understanding the cyber threat to the medical centre and how someone will use the ASMIS system needs to be understood. A Use Case can be graphically represented in a diagram to show a typical use of the system. Figure 1 shows how the ASMIS system is used by prospective patients and the steps that they need to go through to create an account to use the system all the way through to being able to book a specialist for treatment.

Diagram

Description automatically generated

Figure 1 Use Case

Understanding how the ASMIS system is going to be used can then be used to create an abuse case and see what the potential cyber threat is. Figure 2 shows how a malicious staff member could interact with the system to create harm.

Diagram

Description automatically generated

Figure 2 Abuse Case

Understanding how the system works and a possible way the system can be compromised will establish a baseline for work (Firesmith 2003). The report will now show what can be done to understand the risk more and mitigate against them.

First, there needs to be an understanding of the system's data flow for that a Class diagram can be used. The Class diagram displays the structure of a system, their class, attributes and behaviours and the interaction between them.

Figure 3 shows a Class diagram of a user interacting with the ASMIS system. Each rectangle box has three compartments. The top compartment is the class's name, and it is mandatory the bottom two display attributes and operations or behaviours. For example, figure 3 displays the class ‘user’ with some attributes ‘name’, ‘department’ and the operations of ‘logon’, ‘logoff’, and others within the rectangle. The whole diagram shows how the different classes interact with their own attributes and operations. This details how patients goes through the ASMIS system creating an account, detailing their health history and eventually booking a specialist. Along the way, their details would have been checked the specialist allocated, and billing arranged.

Diagram

Description automatically generated

Figure 3 Class Diagram

Once figure 3 has been documented, a threat analysis can be made against it. STRIDE can be used by applying the six principles to figure 3 to understand how the ASMIS system can be attacked. For the Queens medical centre, four of the six threats can be used by the malicious staff member. These include Spoofing, which would involve the malicious staff member falsely identifying themselves as someone else. Tampering would be the staff member gaining access to data and adjusting it for their own means. Information Disclosure would be the staff member sharing that information, and the Elevation of privileges would be the staff member having a higher level of access to the ASMIS system than they should.

This report will set out in figure 4 a way to mitigate the threats by using a behavioural Sequence diagram to combat the perceived threats.

Diagram

Description automatically generated

Figure 4 Behavioural Sequence diagram

Figure 4 shows a behavioural diagram that shows the sequence of interaction from the Class diagram in figure 3. The class headings are shown, and the data flow between each. Understanding the threats from the STRIDE and CIA analysis the behavioural sequence diagram can be created; this will show where security elements can be placed to stop the malicious staff from attacking the system. For example, the user needs to be authenticated four different times, in different ways and to varying depths into the system. If the user passes all four security checks, the specialist is booked and billing raised for the appointment.

In conclusion, the Queens medical centre has acquired a web-based booking system (ASMIS). There is concern over the security and integrity of the system. This report has set out to explore one threat dynamic, that of a malicious staff member. A typical use case of how a potential patient can create an account and book a specialist. Understanding the use case has allowed an abuse case to be explored of how a malicious staff member could exploit vulnerabilities within the system. A Class diagram was created to understand the data flow and interaction between the different class artefacts. Understanding that data flow and performing a STRIDE analysis of the system led to the creation of a Behavioural Sequence diagram. The Behavioural Sequence diagram was used to show the data interactions in a timeline from the user login to the booking of a specialist. It also established where security interactions could be installed to close any vulnerabilities and limit malicious staff's ability to attack the ASMIS system.

Future recommendations would be for further attack profiles to be developed through threat analysis of vulnerabilities from the ASMIS web-based system and its infrastructure. To do that, a greater understanding of the ASMIS system would be required.

References

Booch, G. (1999). *Unified Modeling Language User Guide, The*. 2nd Edition. Addison-Wesley

Firesmith, D. Journal of Object Technology. (2003) Security Use Cases. *Journal of Object Technology* vol. 2 (no. 3): pp. 53-64. Available from: <https://www.researchgate.net/profile/Donald-Firesmith/publication/220298964_Security_Use_Cases/links/0fcfd50f968923098e000000/Security-Use-Cases.pdf> [Accessed 12 March 2021]

Microsoft (2019)  Uncover Security Design Flaws Using The STRIDE Approach Available from:<https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach> [Accessed March 10, 2021]

OWASP (2021a) OWASP TOP TEN. Available from: <https://owasp.org/www-project-top-ten/> [Accessed 10 march 2021]

OWASP (2021b) Abuse Case Cheat Sheet. Available from: <https://cheatsheetseries.owasp.org/cheatsheets/Abuse_Case_Cheat_Sheet.html> [Accessed 10 march 2021]

Yin, L. Change, Z. International Journal of Distributed Sensor Networks (2020) Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks* vo.16 (1): pp. 1-13 Available from: <https://journals.sagepub.com/doi/pdf/10.1177/1550147719899374> [Accessed 10 March 2021]

Walkowski, D. (2019) F5. Available from: <https://www.f5.com/labs/articles/education/what-is-the-cia-triad> [Accessed 20 March 2021]