Threats and Risks Analysis of the Appointment and Scheduling Management Information System (ASMIS)

Raquel Martinez Diez

Introduction

Currently the Queens Medical Centre consultation appointment requests are managed by telephone. This method has proven to have problems as patients report delays in getting appointments with specialists. The proposed solution of a web-based Appointment and Scheduling Management Information system (ASMIS) will introduce important benefits in the appointment process. The system will allow patients to schedule appointments online. With the system, patients will benefit from less time consuming appointment bookings, facilities for appointment modification and cancellation, and the ability to reserve appointments at any time, even outside working hours. For the medical centre, the system will mean paper and money savings, and it is expected that the attendance rate will be improved.

However, following a significant increase of cyber security attacks in recent years, the Management Team is concerned about the security aspects of the system. Common network security measures will be applied to the final system infrastructure, but experience has shown that poorly designed systems are a major cause of security flaws (Hoglund & McGraw, 2004). Rigorous and formal methods for modelling and analysing security aspects offer a solid foundation for achieving a high degree of system security (Wing, 1998). The process of system design and development must include a security threats and risks analysis. Therefore, a security team has been created to participate in the system development process from start to end. It is important to know that the CIA triad is a fundamental part in planning and implementing security policies aimed at keeping data secured (Fruhlinger, 2020). The CIA triad is a widely used information security model that focus on the three principles of Information Security: Confidentiality, Integrity and Availability. From these principles the major concerns for the AMIS system are confidentiality and integrity.

Confidentiality means that data must be protected from unauthorized viewing. For sensitive patient data like the one stored in the AMIS system, privacy settings and access control must have a high level of security. The key to preserving confidentiality is making sure that only authorized individuals have access to the information (Verri Lucca et al., 2020). Enforcing access controls, that is limiting who can see what, is also an essential technique to ensure confidentiality. Another tool is encryption: patient data should be stored and transmitted in encrypted ways, and only the users who have the authorization to view it should be able to decrypt it. Lastly, governmental policies and laws, like the General Data Protection Regulation (GDPR), deal with the need to protect confidential data and the consequences of data theft. Compliance with the GDPR regulation is imperative for the AMIS system as it stores sensitive private information.

Integrity means that data must be protected from deletion or modification by unauthorized users. Data stored in the ASMIS application must be reliable in order to ensure that appropriate care is provided to patients, increase the consistency in treatments and improve patient outcomes. As integrity is also related to data, all efforts applied to preserve confidentiality are valid for preserving integrity as well.

Security Threats and Risk Assessment

Threat modelling is being used in the secure software engineering as a structured way to deliver secure systems. The thread modelling process followed in this document first identifies threats to the system based on application decomposition, then evaluates the identified threats and assesses risks associated with them, and finally chooses assurance techniques to mitigate them (Howard & LeBlanc, 2003). This process also lays the fundamentals for how the risks are monitored and managed while the application is used in production.

Threat Identification

Security threats indicate potential attacks that can be executed in the system. The first step of threat identification is the decomposition of the system into assets, including system components and users. The reason for this decomposition is to identify how the data flows between the different components in order to identify areas to protect. These components should be regarded as threat targets and threats should be considered for each of them. The STRIDE model is extensively used by security designers when considering threats. STRIDE is the acronym of the six categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of privilege. Each threat category breaches one or more principles of the CIA triad.

It is important that users participate in the threat identification process because they are more familiar with the application domain (health in this case) and may anticipate security threats that are not recognized by the security team. To facilitate the user participation and the communication of design decisions, the security team's approach is to use a framework based on the Unified Modelling Language (UML) to represent the system structure and design decisions (Scott, 2003). UML is a visual language used for modelling software artifacts that can encourage user participation. The UML methodology is used in our process as a visual modelling tool to support a rigorous analysis using the STRIDE model. A UML class diagram (figure 1) is used to represent the different objects of the system and sequence diagrams are used to represent system processes (figure 2 represents the booking appointment process). The purpose of these diagrams is to help users understand the information flow in the system and identify threats. A UML misuse case diagram (figure 3) is also used to represent the threats identified in the system. The diagrams included below do not represent the complete system, but are examples to illustrate the approach.

In summary, the steps for threat identification are (1) identification of system components, (2) application of the STRIDE model to each component to consider possible threats, (3) representation of the system using UML diagrams, and finally, (4) identification/validation of threats with users. As the AMIS application is complex, the list of identified threats mentioned in this document is not exhaustive but provides a basis to demonstrate the adopted approach.

The AMIS application has the following main components and users:

Component/User	Comments
User	There are two different user roles: patients and doctors. Patients can enter and view their patient data and can manage their appointments with specialists through dedicated web pages. They cannot access other patient data. Doctors can access their scheduled appointments and all patient data in the system.
Administrator	The administrator is in charge of administering the servers and networks, as well as managing the authentication data.
Website	Access point for users. The interface is implemented with HTML.

Web server	Contains the application code including all the logic.
Patient Data	The patient data sis accessed by the web server to read and write. The data is also transferred to and from the web server and the user interface (website).
Authentication Data	Accessed by the database server and the administrator. Verifies whether users have access to the system and determines user access level.

UML Diagrams

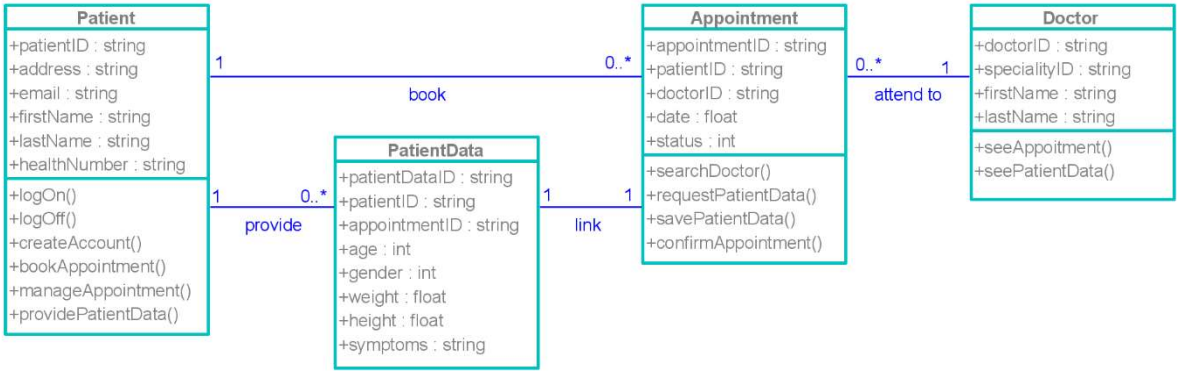

Figure 1 - Class diagram for ASMIS application

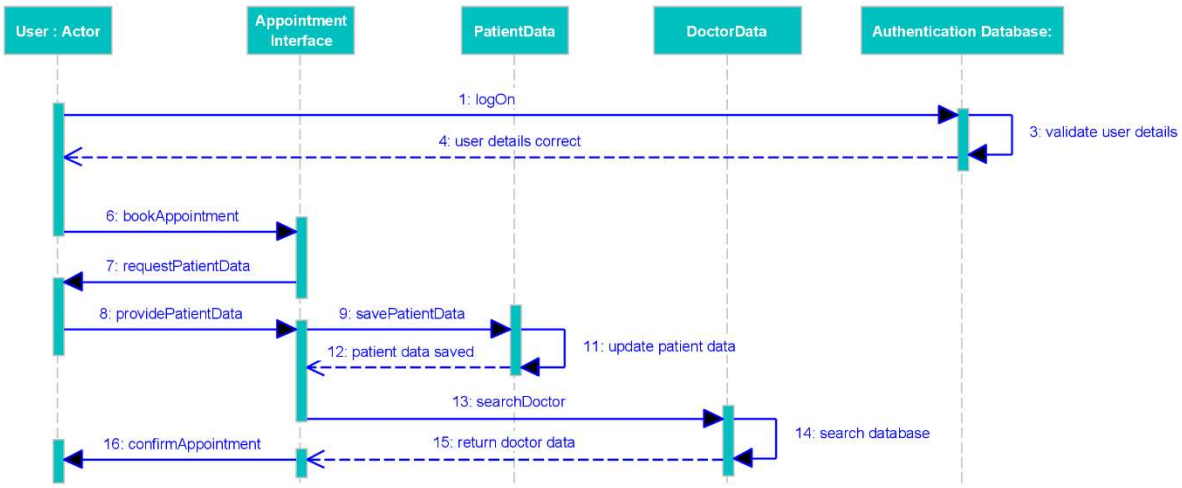

Figure 2 - Sequence Diagram for Book Appointment use case

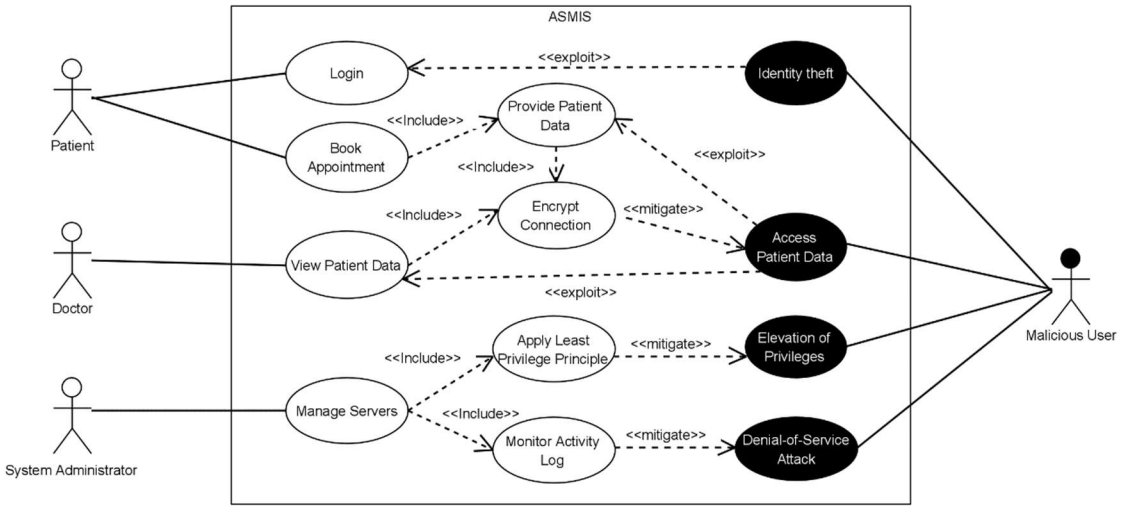

Figure 3 - Misuse case scenario for ASMIS application

Based on the analysis done with the application decomposition and the UML class and sequence diagrams, the security team has identified two main threat targets to protect: (1) the patient data due to its sensitive nature and (2) the web server, as it is in the public domain and the patient data is transmitted through it. For these targets, the following threats have been identified:

ID	Threat Description	Potential Impact
T1	Unauthorized access to patient data during network transmission	This threat affects the data flow between several components. Sensitive data is transmitted from the web server to user clients. During the transmission, the data can be intercepted in different ways. The most common ways are to use a network protocol analyser or to compromise a router to look at the data in transit. If this threat is exploited, it has a very big impact as it means a personal data breach. These breaches are regulated by the GDPR and can have important legal consequences due to the personal damage induced to users (Information Commissioner's Office, n.d.).
T2	Credential theft	The target component of this threat is the user. As explained by Beirstein (n.d.), credential theft allows attackers to have the same account privileges as the victim, thus gaining access to private data. Typical attacks targeting credential theft include fishing, brute force attacks (trial and error method) and attacks taking advantage of weak or insecure authentication protocols. The exploit of this threat could have the same impact as T1, depending on the access level of the user.
T3	Attacker denies service to application	The web server is in the public domain and can be targeted by Denial-of-Service attacks (DoS). DoS attacks are quite common and, therefore, protection measures must be taken. DoS attacks can be achieved by flooding the target server with traffic or sending information that triggers a crash. The consequence is that legitimate users are deprived of the service they expect. Furthermore, this threat violates the data availability principle of the CIA triad, which makes the impact of the threat more significant.

T4	Attacker elevates privilege through web server	The target for this threat is again the web server. These threats happen when attackers exploit bugs, design flaws or configuration errors in applications or in the operating system to gain access to restricted resources. An attacker with elevated privileges, can run administrative commands or deploy malware, and make serious damage to the organisation IT infrastructure making the impact of this attack quite serious.

Threats and Risks Assessment

A risk is essentially the organisational exposure generated by the probability and potential impact of a threat materializing itself (Government of Alberta, 2018). In this document, risks are assessed by multiplying the probability (P) factor (1-10) with the impact (I) factor (1-10) to obtain the overall exposure (E=P*I) factor (1-100), which is used to assign a priority to the various identified threats. Once risks have been categorised, a decision has to be taken on how to respond to each risk. Risk responses need to be discussed and agreed with the Management Team. The risk responses follow the PRINCE2 classification (Office of Government Commerce, 2009):

- Accept the risk and do nothing to mitigate it.
- Mitigate the risk by either developing a mitigation plan or by implementing a measure to reduce the probability and/or the impact of the risk.
- Avoid the risk by discontinuing activities that are generating the risk.
- Transfer or share the risk by transferring all or part of the impact of the threat to a third party.

The following table shows the risk assessment performed by the security team:

ID	Threat Description	P	I	E	Treatment/Response
T1	Unauthorized access to patient data during network transmission	7	10	70	ACTION: Mitigate This threat can be mitigated using the Transport Layer Security (TLS) protocol to ensure traffic is protected. This protocol is used to encrypt data between the web server and the client.
T2	Credential theft	8	9	72	ACTION: Mitigate Using strong authentication methods could mitigate this treat. Instead of single authentication, the benefits of multi factor authentication methods should be considered. Preventive measures can also be applied by creating a security awareness culture in the medical centre with information campaigns and user training about security threats, including credential theft methods.
T3	Attacker denies service to application	7	6	42	ACTION: Mitigate There are two measures proposed to mitigate this threat. Apart from applying common network security practices, including firewall and restricted access to resources, a DoS attack response plan will be developed in order to minimise the impact of an eventual attack.
T4	Attacker elevates privilege through web server	2	10	20	ACTION: Mitigate To mitigate this threat a strong access control at all levels is necessary by applying the least privilege

					principle to user accounts, especially those with high privileges, and by applying IP restrictions to the web server. Another measure is to ensure that database and application development follow best practices to avoid common features exploited by attackers.

Security Measures

Effective network security requires a combination of protection tools such as firewalls, anti-malware, intrusion prevention or application security. The firewall is a fundamental protection technology used for securing network infrastructure. The purpose of firewalls is to protect internal networks from attacks originated on the Internet by filtering incoming and outgoing traffic based on a predefined criteria such as IP addresses, packet type or port number (Forcepoint, n.d.). However, one limitation of basic firewalls is that they inspect the source and destination IP addresses to determine if packets are safe but cannot check if the packet contains malicious code. New-Generation Firewalls (NGFW) have advanced security features such as application-level inspection to detect and block risky applications, intrusion prevention and threat intelligence. These features provide NGFWs with the ability to detect and block threats like advanced malware and application layer attacks, thus improving defence capabilities against DoS attacks.

To ensure secure communication over the Internet, encryption of data in transit is necessary. If data is not encrypted, attackers can survey the transmission and read confidential information. The TSL protocol provides end-to-end communications security over the Internet. TLS encrypts all types of Internet traffic, including web traffic. Today it is widely used by organisations to encrypt their web traffic. TLS ensures data integrity and authenticity by providing strong message authentication. During the communication, the TLS first uses the handshake protocol to check the message authenticity using asymmetrical cryptography (public/private key pairs) and then the records protocol to transmit the message and check its integrity symmetrical cryptography (shared key). The security benefits of the TSL justify the adoption for the ASMIS application.

The GDPR requires the confidentiality of patient data. Cryptography is a critical tool when dealing with personal information. In the ASMIS application cryptography methods must be implemented as patient data is by definition personal information and must be kept private. Patient data must be stored in encrypted ways, so that only authorized users, who have a secret key, can decrypt and access it. Encryption of stored data (at rest) is a key protection feature against a data breach. Popular encryption methods include Advanced Encryption Standard (AES) or RSA.

Finally, a security awareness campaign will have to be developed and carried out in the medical centre once the system is production. Moreover, a DoS response strategy will be formulated in order to minimize the impact a potential DoS attack.

REFERENCES:

Berstein, C. (n.d.) Credential theft, definition. Available from: https://searchsecurity.techtarget.com/definition/credential-theft [Accessed 27 March 2021].

Government of Alberta (2018) Security Threat and Risk Assessment (STRA). Available from: https://imtpolicy.sp.alberta.ca/procedures/Supporting%20Documents/Security_Threats_and_Risks_Assessment_Template.docx [Accessed 27 March 2021].

Information Commissioner's Office (n.d.) Personal data breaches. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches [Accessed 26 March 2021].

Forcepoint (n.d.) What is a Firewall? Firewalls defined, explained, and explored. Available from: https://www.forcepoint.com/cyber-edu/firewall [Accessed 28 March 2021].

Fruhlinger, J. (2020) The CIA triad: Definition, components and examples. Available from: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html [Accessed 24 March 2021].

Hoglund, G. & and McGraw, G. (2004) Exploiting Software: How to Break Code. Addison-Wesley.

Howard, M & LeBlanc, D. (2003) Writing secure code: practical strategies and proven techniques for building secure applications in a networked world. 2nd ed. Redmond, Wash: Microsoft.

Office of Government Commerce (2009) Managing Successful Projects with PRINCE2: 2009 Edition. 2009th ed. Stationery Office Books.

Scott, W. (2003) The Elements of UML™ Style. Ambler.

Verri Lucca, A., Augusto Silva, L., Luchtenberg, R., Garcez, L., Mao, X., García Ovejero, R., Miguel Pires, I., Victória Barbosa, J. & Quietinho Leithardt, V. (2020) A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information. Sensors (Basel). 2020;20(21):6030. Available from: https://www.mdpi.com/1424-8220/20/21/6030 [Accessed 23 March 2021].

Wing, J. (1998) 'A Symbiotic Relationship Between Formal Methods and Security', in: The Proceedings of the Workshops on Computer Security, Dependability, and Assurance: From Needs to Solution. 26-38.