Queens Medical Centre (a community clinic) has decided to acquire a web-based appointment and scheduling management information system (ASMIS). The system will facilitate online appointments made by patients to doctors based on their speciality. The objective of this paper is to provide a holistic approach to cybersecurity concerns, potential threats, and mitigation techniques for the ASMIS to ensure that the system is secure. The benefits of the ASMIS as well as cybersecurity technologies used to mitigate threats will be critically analysed and discussed. Recommendations will be provided to ensure that the system is deployed, maintained, and supported in a secure manner.

In contrast to the traditional telephonic appointment booking method, a web-based appointment and scheduling system allows prospective patients to book appointments online by selecting the most favourable slot available. The benefits of such a system include 24-hour booking convenience, reduction in scheduling delays as well as a reduction in patient waiting times (Akinode, 2017). Furthermore, Zhao et al. (2017) mentions the following benefits: reduced no-show rate, time saved for specialists, receptionists, and patients, decreased staff labour as well as an improved satisfaction amongst patients. Lowes (2004) discusses an added benefit where patients can be pre-screened, review clinic policies and complete registration forms online prior to their appointment. Walters et al (2003) reported that “Patient Online”, a web-based scheduling system reduced no-shows by 42%. While the benefits are evident, online systems also have the capability of storing sensitive patient information. Patients were found to be reluctant to share medical details when interacting with an online system (Zhao et al., 2017). Handling sensitive and personal data over the internet gives rise to several possible cybersecurity concerns.

Cybersecurity concerns can be considered as an approach to ensure Confidentiality, Integrity and Availability (CIA) of information. Confidentiality refers to the controlled access to information, Integrity refers to data that should not be altered in any way and Availability refers to the reliability and uninterrupted access to data (Samonas & Coss, 2014). Singh et al. (2014) mentions the following threats to systems in accordance with the CIA triad:

Confidentiality – snooping (capturing data without access rights) and traffic analysis (monitoring network traffic) are two types of attacks that threaten confidentiality. Integrity – modification of data by hackers. Availability - DDOS (Distributed Denial of Service) attacks causing systems to become unresponsive and unable to perform its desired function.

To visually depict threats to a system, a modelling language is used. UML (Unified Modelling Language) is used to model security threats to the ASMIS. According to Kong et al. (2010: 876) “UML is a widely applied standard language for visually modelling object-oriented systems”. UML diagrams presents a common framework for modelling and analysing security threats visually (Kong et al., 2010).

Figure 1 below represents a class diagram with various classes of the ASMIS. These classes store relevant information of the ASMIS.

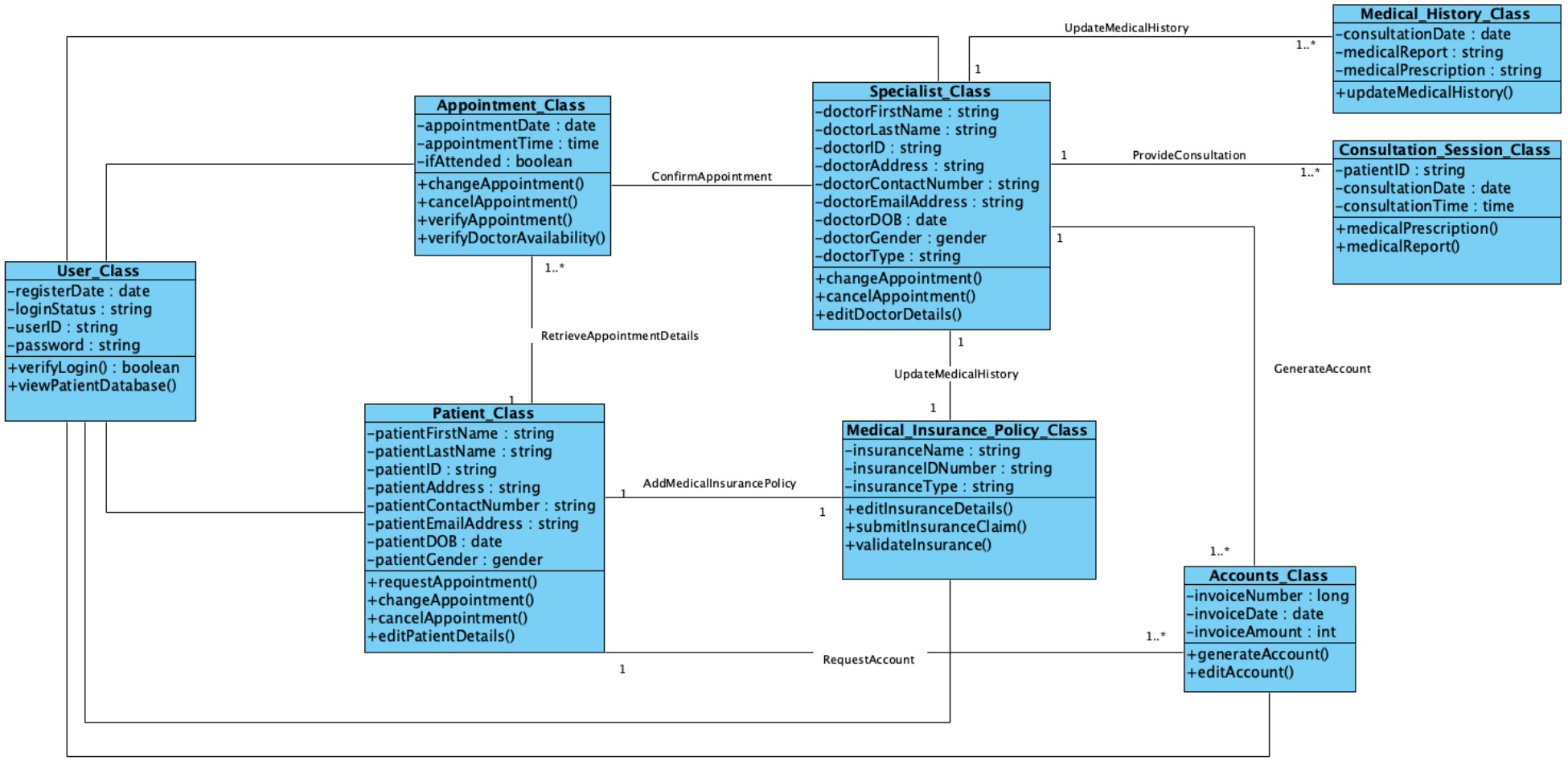

Figure 1: Class diagram (ASMIS)

When prospective patients visit the ASMIS, they will follow a normal website behaviour such as completing a user registration, logging in and scheduling an appointment with a specialist as depicted in Figure 2 below. Malicious users or attackers on the other hand will tend to utilize attack tools to brute force the system as well as try to locate server vulnerabilities and exploit them. The objective of performing such attacks is to gain access to private sensitive information (Gao et al., 2017).

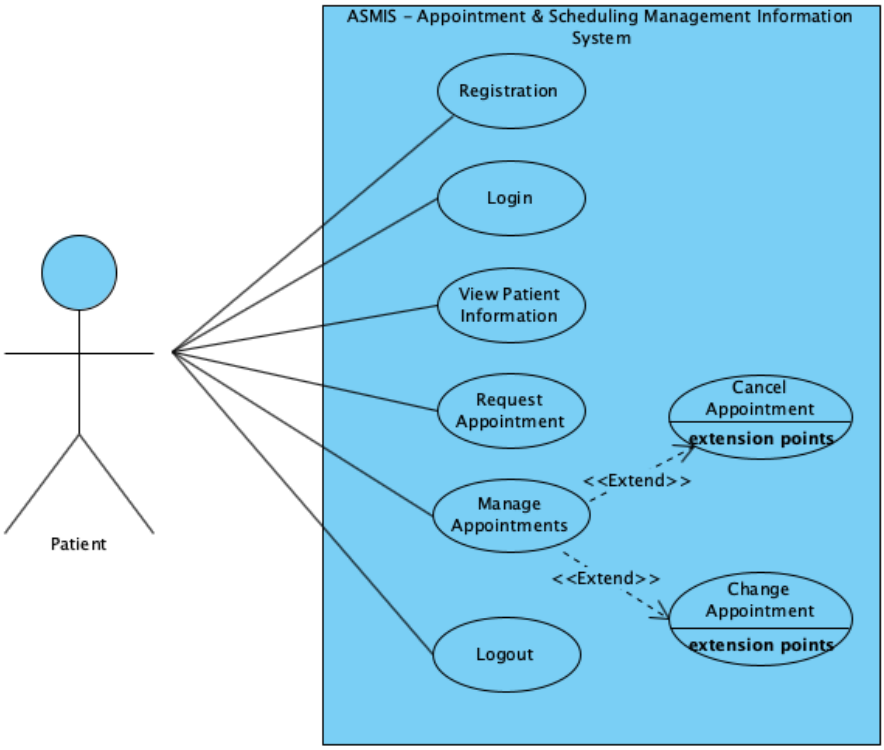

Figure 2: Patient - Use Case (ASMIS)

Internal users are users that are given access to the system to perform their daily function. An internal non-malicious user is allowed to search and update patient and medical history records as well as accept appointments. Internal users may also generate account bills depending on the level of access they have. Figure 3 below represents a use case for an internal non-malicious user (receptionist/specialist). Internal users pose a far greater threat if they are to be malicious. A malicious user can delete patient records, sabotage appointments as well as leak medical history and account information; this abuse case is represented in Figure 4 below:

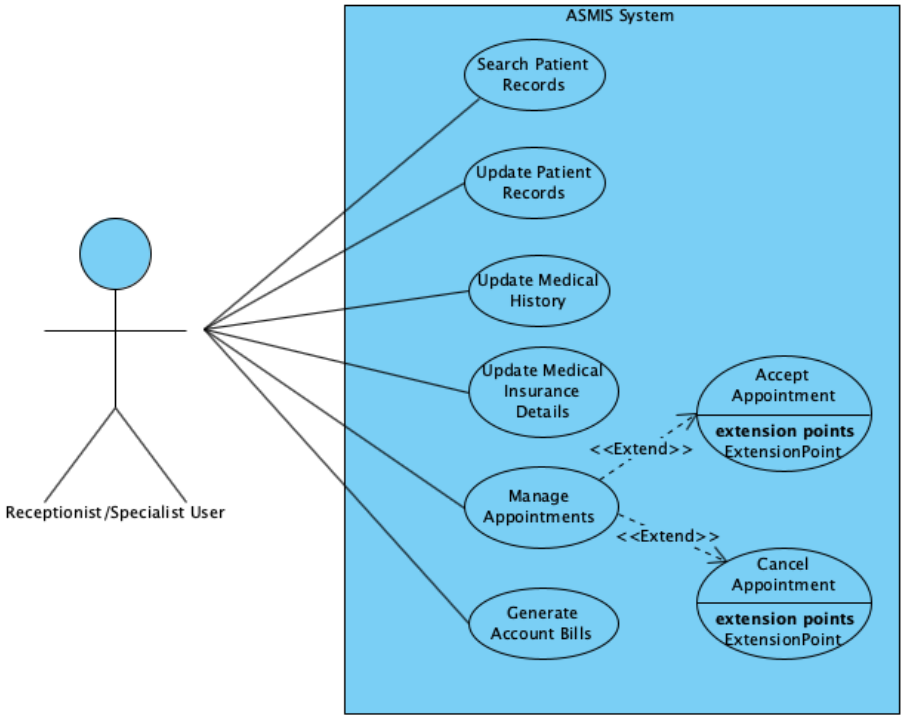

Figure 3: non-malicious user - Use Case (ASMIS)

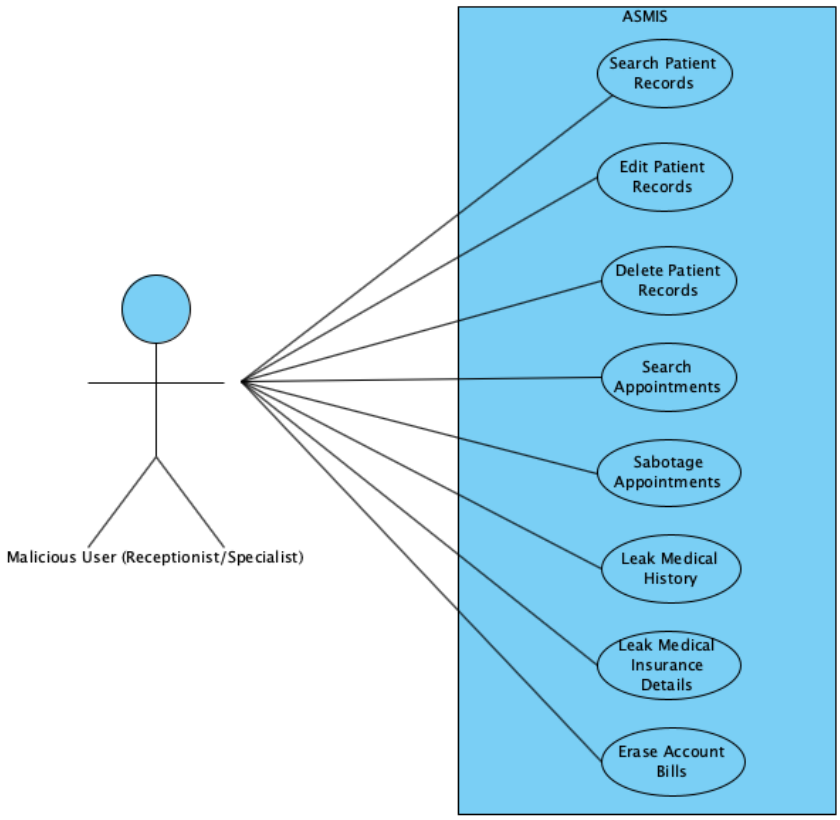

Figure 4: Malicious User - Abuse Case (ASMIS)

Threat modelling techniques are often used to identify threats to a system. A common threat modelling technique called STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is used to model security threats in ASMIS (Howard & Leblanc, 2003). The following section will outline threats as well as possible security technologies used to mitigate these threats in line with the STRIDE technique.

Spoofing – Allows a hacker to masquerade as another user to gain access to a system. Spoofing can be carried out using phishing attacks, pretexting or in the form of spam e-mails. Phishing refers to a technique which involves sending e-mails, that look like company legitimate e-mails to deceive recipients to disclose personal information or passwords to systems (Anderson, 2020). Pretexting refers to a technique that involves an attacker pretending to need information to successfully confirm the identity of a person (Anderson, 2020). The human element is said to be the weakest link in these types of attacks (Tsochev et al., 2020). The above-mentioned attacks can be used to successfully obtain passwords and gain access to the ASMIS. Protection against phishing attacks is enhanced by security awareness and training provided to end users. Staff need to attend mandatory security awareness training that explains the importance of reading e-mails carefully as well as verifying its source.

Furthermore, random phishing e-mail simulations can be performed by the cybersecurity teams. This will provide an indication of which users are still inclined to clicking on suspicious links from unknown sources. Further protection exists in the form of end-point security technologies such as Antivirus software, anti-malware, and firewalls; these technologies should be installed at Queens medical centre. While end-point security technologies do not offer complete protection since virus's evolve, the chances of systems becoming infected will be significantly reduced (Tsochev et al., 2020).

Spoofing can also be applied in a data centre access context, if strict access control policies and procedures are not in place, attackers can pose as employees to get access to servers hosting the ASMIS application.

Tampering – Involves the modification of data. This coincides with data Integrity, part of the CIA triad mentioned previously. As depicted in Figure 4 - patient data can be edited and deleted by employees with malicious intent using the ASMIS. Grispos et al. (2019) argues that date, time, consistency, and completeness of data are vital when carrying out security investigations. In addition, regulations such as GDPR (General Protection Data Regulation) should also be considered which mandates core data principles such as accuracy, storage limitation, purpose limitation amongst others (GDPR, 2021).

An Identity and Access Management (IAM) system should be implemented to control access to the ASMIS. IAM includes Role Based Access Control (RBAC) which restricts access based on a person's role in an organisation as well as Multi-Factor Authentication (MFA). MFA was designed to provide a higher level of safety and protection to systems, while also providing a resilient way of authenticating users (Dasgupta et al., 2017). MFA includes three types of authentications i.e., password, smartphone pin as well as a biometric factor (fingerprint, face recognition, etc). Users should be required to comply with a strict password policy which includes a minimum length of 16 characters, a mixture of upper- and lower-case letters as well as special characters to gain access to the ASMIS. In addition, a Time-Based One-Time Pin (TOTP) application can be installed on user's smartphone to comply with the MFA requirement. Hamza (2011) mentions that with the implementation of an IAM system the challenges of maintaining credentials and multiple identities across systems in a network is reduced. In contrast, Mohammed (2019) argues that companies should not rely on IAM to prevent unauthorized usage on systems; policies should be configured carefully to align with the roles of staff.

Repudiation – Involves the clearing of log activity once a system is hacked (Howard & Leblanc, 2003). Hackers clear log files to eradicate their footprints. All logging information from various devices on the network hosting the ASMIS should be sent to an external monitoring and logging system. An Intrusion Detection System (IDS) should be implemented at the clinic which detects and alerts of malicious activity (Tiwari, 2017). An IDS will screen incoming requests to the ASISM; this will aid the cybersecurity team at the clinic to detect, troubleshoot and mitigate any possible attacks on the ASMIS. In contrast, according to Vigna et al. (2003) IDS's are based

on simple pattern matching techniques in HTTP requests which are often missed by default IDS configurations.

Information Disclosure – Involves the exposure of information that does not belong to the person exposing it (Howard & Leblanc, 2003). If hackers gain access to the ASMIS, sensitive patient and specialist information can be exposed. Information stored in the ASMIS database should be encrypted and access to the database should be limited according to permissions configured in the IAM system.

Denial of Service – DOS attacks on a system make it unresponsive and unusable. The objective of a DOS attack on ASMIS would be to prevent users from accessing the system and therefore sabotaging the operations of the clinic. Next Generation Firewalls (NGFW) play a vital role in protecting companies against evolving and sophisticated threats as well as DOS attacks. Vendors such as Palo Alto, Fortinet and Checkpoint Software Technologies remain leaders in producing NGFW's with advance features such a IPS (Intrusion Prevention System) and identity awareness (Gartner, 2020). In addition, Soewito & Andhika (2019) prove that NGFW's are effective against DDOS, phishing and SQL (Structured Query Language) injection attacks through various experiments performed on corporate networks. To protect the ASMIS against DDOS, SQL injection, XSS (Cross-Site Scripting) and cookie poisoning amongst others, the implementation of a NGFW as well as a Web Application Firewall is necessary. SQL injection is achieved by injecting SQL code into a database. XSS attacks are achieved by injecting malicious code into a web browser and cookie poisoning is achieved by hijacking a user's session (F5 Inc, 2021). Both technologies (NGFW and the WAF) are required as they offer protection at different layers i.e., the NGFW will offer protection at the edge of the network while the WAF will provide protection to the ASMIS application (F5 Inc, 2021). The drawbacks of these technologies include cost (expensive to implement) as well as an impact on performance. Packet inspection is necessary for these technologies to be effective and will therefore slow down the network. Babiker et al. (2018) further argue that WAF's produce high false negatives and are unable to detect unknown attacks.

Elevation of Privilege – This involves a user (external or internal) that had restricted access and has gained privileged access sufficient to break the system (Howard &

Leblanc, 2003). Attackers usually exploit vulnerabilities, misconfigurations, or erroneous access controls to escalate privileges. Mitigation techniques such as network segregation (domains and subdomains), penetration testing, patching vulnerabilities as well as operating system hardening techniques can be implemented on the ASMIS network. The objective of network segregation would be to isolate attacks and stop threats from spreading across the network. Patching processes must be defined to ensure systems are patched regularly or according to a schedule. Regular penetration testing must be performed on all applications and servers in the ASMIS network to ensure vulnerabilities are identified and remediated. Operating system hardening techniques should also be implemented in line with vendor recommendations to ensure that systems remain secure.

Figure 4 below represents a malicious staff sequence diagram of the ASMIS with inbuilt security. The system allows staff to authenticate via Multi-Factor Authentication as well as depicts various Role-Based Access Control mechanisms.

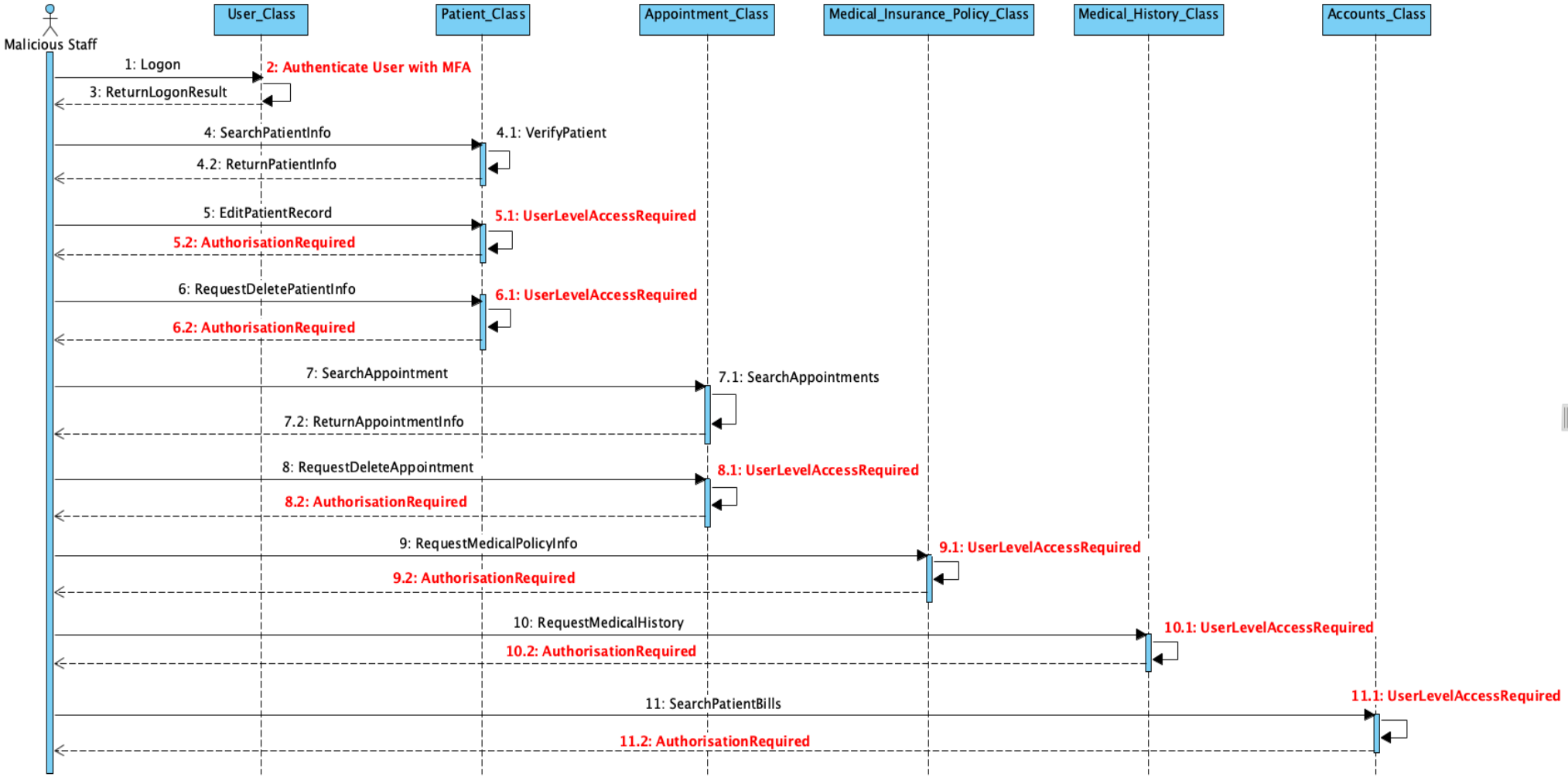

Figure 5: Malicious Staff Sequence Diagram (Inbuilt-Security)

The Cyber Security Breaches Survey 2020 confirms that data breaches are on the increase. It is therefore vital that the clinic implements security technologies, policies, and controls to minimize data breaches and protect the ASMIS. While the recommended security technologies will not ensure that the ASMIS is 100% cyber-attack proof (VanSyckel, 2018); it offers protection to many known attacks and are still required as a first layer of defence. Queens medical centre will need to adopt various security technologies to ensure that networks remain protected end-to-end. It is also important to understand cyber risks as well as create a cybersecurity culture within the clinic that shares a common way of thinking amongst users; this will ensure that security across the clinic is enhanced and subsequently lead to a decrease in the number of cyber-attacks (Boehm et al., 2019).

List of References

Akinode, J, L & Oloruntoba, S, A. (2017) Design and Implementation of a Patient Appointment and Scheduling System. *International Advanced Research Journal in Science, Engineering and Technology,* 12(4): 16-23. Available from: https://www.researchgate.net/publication/332864696_Design_and_Implementation_of_a_Patient_Appointment_and_Scheduling_System [Accessed 03 October 2021].

Anderson, R. (2020) *Security engineering: a guide to building dependable distributed systems.* 3rd ed. Indiana: John Wiley & Sons Inc.

Babiker, M., Karaarslan, E., Hoscan, Y. (2018) 'Web application attack detection and forensics: A survey', *6th international symposium on digital forensic and security (ISDFS).* Turkey, 22-25 March 2018. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/8355378 [Accessed 09 October 2021].

Boehm, J., Curcio, N., Merrath, P., Shenton, L., Stahle, T., McKinsey & Company. (2019). *The risk-based approach to cybersecurity*. Available from: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity [Accessed 10 October 2021].

Department for Digital, Culture, Media & Sport (2020) *Cyber Security Breaches Survey 2020.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf [Accessed 09 October 2021].

F5 Inc. (2021) WAF vs. NGFW: Which Technology Do You Need?. Available from: https://www.f5.com/c/landing/waf-vs-ngfw-which-technology-do-you-need [Accessed 09 October 2021].

Gao, Y., Ma, Y., Li, D. (2017) 'Anomaly detection of malicious users' behaviors for web applications based on web logs', *17th International Conference on Communication Technology (ICCT)*. China, 27-30 October 2017. USA: IEEE.

Gartner. (2020) Gartner Magic Quadrant for Network Firewalls. https://www.gartner.com/en/documents/3992870. [Accessed 08 October 2021].

GDPR. (2021) General Data Protection Regulation (GDPR). Available from: https://gdpr-info.eu/ [Accessed 05 October 2021].

Dasgupta D., Roy A., Nag A. (2017) *Multi-Factor Authentication. In: Advances in User Authentication*. 1st ed. New York: Springer Publishing. Available from: https://doi.org/10.1007/978-3-319-58808-7_5 [Accessed 04 October 2021].

Grispos, G., Glisson, W.B., Storer, T. (2019) 'How good is your data? Investigating the quality of data generated during security incident response investigations', *The 52nd Hawaii International Conference on System Sciences (HICSS-52)*. Hawaii, 11 January 2019. USA. Available from: https://arxiv.org/abs/1901.03723 [Accessed 05 October 2021].

Hamza, M, K., Abubakar, H., Danlami, Y, M. (2018) Identity and Access Management System: a Web-Based Approach for an Enterprise. *Path of Science*, 4(11): 2001-2012. Available from: https://cyberleninka.ru/article/n/17882812 [Accessed 05 October 2021].

Howard, M & Leblanc, D, E. (2003) *Writing Secure Code*. 2nd ed. Redmond, WA, USA: Microsoft Press.

Kong, J., Xu, D., Zeng, X. (2010) UML-BASED Modelling and Analysis of Security Threats, *International Journal of Software Engineering and Knowledge Engineering,* 20(6): 875-897. Available from: https://www.researchgate.net/publication/220344852_Uml-Based_Modeling_and_Analysis_of_Security_Threats [Accessed 05 October 2021].

Lowes R. (2004) Phones driving you crazy? Try clinical messaging. *National Library of Medicine,* 81(6): 65-76. Available from: https://pubmed.ncbi.nlm.nih.gov/15077492/ [Accessed 04 October 2021].

Mohammed, I, A. (2019) Cloud Identity and Access Management – A model proposal. *International Journal of Innovations in Engineering Research and Technology*, 6(10): 1-8. Available from: https://repo.ijiert.org/index.php/ijiert/article/view/2781 [Accessed 07 October 2021].

Samonas, S. & Coss, D, L. (2014) The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, 10(3): 21-45. Available from: http://www.proso.com/dl/Samonas.pdf [Accessed 04 October 2021].

Singh, A., Vaish, A., Keserwani, K, P. (2014) Information Security: Component and Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(1): 1072-1077. Available from: https://www.academia.edu/download/44838850/Information_Security_-_Component_and_Techniques.pdf [Accessed 04 October 2021].

Soewito, B & Andhika, C, E. (2019) 'Next Generation Firewall for Improving Security in Company and IoT Network', *2019 International Seminar on Intelligent Technology and Its Applications 2021(1):* 205-209. Available from: https://sci-hub.se/10.1109/ISITIA.2019.8937145 [Accessed 08 October 2021].

Tiwari, M., Kumar, Raj., Bharti, A., Kishan, J. (2017) INTRUSION DETECTION SYSTEM. *International Journal of Technical Research and Applications*, 5(2): 2320-8163. Available from: https://www.researchgate.net/publication/316599266_INTRUSION_DETECTION_SYSTEM [Accessed 07 October 2021].

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., Pavlova, G. (2020) 'Cyber security: Threats and Challenges', *International Conference Automatics and Informatics (ICAI*). Bulgaria, 1-3 October 2020. USA: IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/9311369 [Accessed 05 October 2021].

VanSyckel, L. (2018) Sealevel Systems White Paper - Introducing Cybersecurity. Available from https://www.sealevel.com/support/white-paper-introducing-cybersecurity/ [Accessed 08 October 2021].

Vigna, G., Robertson, W., Kher, V., Kemmerer, R, A. (2003) 'A stateful intrusion detection system for World-Wide Web servers', *19th Annual Computer Security Applications Conference*. Las Vegas, 8-12 December 2003. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/1254308 [Accessed 09 October 2021].

Walters B, A & Danis K. (2003) 'Patient Online at Dartmouth-Hitchcock - interactive patient care web site', *AMIA Annual Symposium*. Washington, 8 December 2003. USA: National Library of Medicine. Available from: https://europepmc.org/article/MED/14728547 [Accessed 04 October 2021].

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B.J., Simoes, E. (2017) Web-based medical appointment systems: A systematic review. *Journal of medical Internet research*, 19(4): 134-143. Available from: https://www.jmir.org/2017/4/e134/PDF [Accessed 03 October 2021].