TITLE: An essay report on ASMIS cybersecurity solutions for Queen's Medical Centre.

Contents

ABSTRACT

Queen's Medical Centre has installed a web-based appointment and scheduling management information system (ASMIS) due to the demands placed upon the medical centre by the neighbouring catchment area of people. The aim is to maximise efficiency to reduce waiting times, provide quality service, and manage staff workloads. The system will permit online appointment booking; however, data protection is a crucial area of concern.

INTRODUCTION

This report aims to provide critical analysis and evaluation of networks, software and human factors that encompass the incorporation of the ASMIS. UML diagrams, threat modelling techniques and cyber security technologies will support findings to address

the concerns and threats raised and maintain the CIA triad of Confidentiality, Integrity and Availability (National Cyber Security Centre, 2018).

DISCUSSION: NETWORKS

Considering networking, the ASMIS offers numerous benefits. The introduction of the system allows incorporating a Wide Area Network (WAN) (Brookshear et al., 2020) to provide ease of access. Patient record data can be viewed and transferred, subject to an elevation of privilege, nationally to which health authorities and boards can communicate efficiently with the local medical centre. Referrals for specialist treatment and updated medical records will be accessed by users with permitted access to care for patients. The Local Area Network (LAN) further compliments CIA by including operation security (Anderson, 2008). Operation security aims to make service disruption difficult, and attackers can only target parts of the ASMIS that are reachable. As Anderson (2008) suggests, operational security is not enough for rules concerning the system. Once access level privilege is issued, staff need education and training to comprehend rules and procedures, particularly data protection.

An additional benefit is interprocess communication (Brookshear et al., 2020). With this approach, we understand the use of the client/server model, which significantly benefits the personnel staff for managing duplicates of patient records. A high capacity mass storage system (file server) can hold all the data needed, and other machines within the network can request access to the records. Staff workload and time management are eased, offering a more outstanding quality of care and service.

When viewing (Appendix 1.1) use case diagram (Ambler, 2005) with an inbuilt design, the advantages are clear to all users of the ASMIS. Authentication is a crucial aspect

so that privileged access of data is provided to the user with a sufficient access level granted by authorisation.

However, we must also consider the problems that can arise with networks. Using the STRIDE threat model (Howard et al., 2014), we can determine the certainty to which threats can occur. The elements that could be affected are spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.

The suggestion of a WAN and or LAN breach would have far-ranging grave consequences for many patients, involving death should network failure or emergency medical treatment be stopped. Anderson (2008) highlighted that a Denial of Service (DoS) attack would be significant enough to halt medical urgent medical treatment. A Distributed Denial of Service (DDoS) attack would shut down services and operations. Severe disruption to services similar to the NHS example in 2017 (Acronis, N.D.) where the EternalBlue software vulnerability shut down processes for several days. The NHS were exploited through a ransomware case known as 'WannaCry", which was delivered via emails through phishing techniques; once activated can lock and encrypt files until the ransom is provided. Threat actors can use social engineering techniques such as this to cause severe problems for the ASMIS. Anderson (2008) also notes that Man In The Middle (MITM) attacks can be exploited through tactics of SYN-flooding. The SYN-flooding tactic is an effective threat, particularly as client addresses can be spoofed, so the cybercriminal may gain an opportunity to compromise the network and perform a MITM attack, causing a data breach.

As highlighted, the interprocess communication that supports the collection and accessibility of patient records is a valuable tool via the client/server method; however, if there is a printer connected, likely for printing records, there is also a problem. Vulnerabilities such as the PrintNightmare (Zarinkhou et al., 2021) can allow threat

actors to execute remote code and the ability to gain local system privileges (Abrams, 2021).

Criminal activity can be visualised in (Appendix 2.4) whereby see an abuse case model. In this case, we view the threat actor using brute force to gain access to the system. The aim could be obtaining admin credentials to infiltrate the system. Repeatedly following this method could lead to further disruption, such as a DoS attack (Nsrav, N.D.). Concerning STRIDE, when considering this UML diagram, we can infer spoofing, tampering, elevation of privilege and denial of service are all threat elements that affect the CIA triad. Spoofing would employ fake IP addresses or credentials to gain access threatening authentication; Tampering would be editing or deletion of medical data records; Denial of Service could occur by the flooding of TCP communication requests to overwhelm the server; Elevation of privilege would occur through gaining authorisation to levels of restricted access.

DISCUSSION: SOFTWARE

The software provides many benefits for ASMIS. As indicated by Anderson (2008), patient records can be anonymised through the use of encryption. This can be very useful to protect sensitive data, and the data could be used for medical research in the future if anonymised, which is helpful for data confidentiality protection. The fundamental principles should be that encryption keys should be kept secret, not open to modification, appropriate length such as AES-192 and encrypt all copies of data (Stine & Dang, 2011). Whilst providers opt for encryption; it does not always consider a complete proof method due to human factors. Access control is essential as staff could leak encryption keys due to negligence or malicious efforts, which would render the security measure useless (Miller & Tucker, 2011). Therefore, medical research

can become more costly (Anderson, 2008) for recovery or further preventative measures.

Software can support efficiency and easy accessibility. Web-based applications can support patient data and drug directories being accessible from home for doctors. Also, functionality can allow medical staff to focus on their specialism, so the quality of care is not compromised. Software technology can improve overall performance (AlHajeri et al., 2021). In contrast, accessibility raises concerns about whether the drug directories are exactly accurate as published by health boards and if doctors have suitable authentication methods and encryption tools to view data from their own homes (Anderson, 2008).

We can consider the behaviour of the cybercriminal in a sequence diagram (Ambler, 2005) in (Appendix 2.2) and understand the extent of the threat posed. The cybercriminal would use the brute force method and hope to pass the authentication stage as the administrator, patient or personnel. When considering STRIDE, we can deduce that STIDE all can be threats when referring to (Appendix 2.2). This sequence diagram shows that the inbuilt design would deny the cybercriminal at the authorisation stage. However, suppose a threat actor was successful in gaining access through spoofing to achieve authentication. In that case, we could see SQL injection attacks on the database, which are common medical attacks (Beavers & Pournouri, 2019), suggesting that tampering could be involved.

Due to negligence or malicious staff, information disclosure could be mitigated through effective policy, procedure, and training. The user details of the database must be protected, and malicious attempts must be controlled. Denial of service can occur once an attacker penetrates the system and denies the users functionality of the software.

The threat actor gains access to additional rights and privileges by achieving malicious breakthroughs, leading to tampering or a data breach.

DISCUSSION: HUMAN FACTORS

Human factors play a significant role in the security of the ASMIS, as previously highlighted; however, access control is a crucial component. Referring to (Appendix 1.2), we can see that the staff can access secure patient records. Data confidentiality is established within access control, and GDPR (Consulting., 2019) will conform the system to laws. The ASMIS eases the manual administration workload, sharing reports with patients and privileged users who require access, such as linked departments or health authorities (Sharma, 2021). The ASMIS will allow patients to access appointment availability (Appendix 1.3), receive appointments notifications, notifications of medicines, request medical certificates, and enable payments for service. Therefore waiting times are reduced, and the service is not overrun (Bankole, 2019). The notion that attendance can improve if booked online due to the user's empowerment is another benefit (Parmar et al., 2009).

Despite the benefits, usability can cause issues. Mismanagement of records or service functionality could occur, resulting in the requirement of sufficient training and accurate staff data input. Patient records can be challenging to secure as doctors and nurses can frequently move roles or departments (Anderson, 2008), which suggests personnel have a high trust elevation due to their privileged access to safety and privacy.

Considering STRIDE further with the TID aspects, there may be disgruntled staff who may act maliciously to delete, copy, modify, disclose data or block system access (Center, 2015), as we can see in the abuse case (Appendix 2.3). In (Appendix 2.1) we

observe the behaviour of a malicious staff user. Despite the inbuilt design, the threat is far greater in contrast to (Appendix 2.2) the cybercriminal. The malicious staff may have specific access level privileges meaning they could infiltrate greater levels of data. At Point 7 (Appendix 2.1), you would consider that the user's verification process may deny further tampering; however, if access controls are not addressed, the staff member may access database records depending on their privileged level. Appendix 1.2 highlights the risk of scale and opportunity of threat that departmental staff could act maliciously.

Cybercriminals can socially engineer an attack through phishing, pretexting, socio-technical USB malware devices or communication approaches (Patel, 2020). These methods prey on vulnerabilities of psychological weakness and can have harmful effects on users social and professional lives, whether a patient or medical staff.

FINDINGS: MITIGATION AND SOLUTIONS

Concerning networks, the use of a Next-Generation Firewall could prove an effective measure. NGFWs can simplify compromise detection and offer a more granular approach to access and controls for specific users (Thomason, 2012). They will monitor traffic activity with deep packet inspection and provide advanced logging to nullify malicious repudiation activities effectively. Administrators workload is alleviated by the inclusion of intrusion detection (IDS) and prevention (IPS) that can alarm administrations of suspicious activity whilst the IPS can drop packets. The disadvantage to NGFWs is that they are expensive and can result in many false-positive and false-positive alerts. They are costly to administer by taking up many system resources to degrade network performance (Mitra, 2017). With many linked network security controls, offering this solution on a single device may be a risk.

In software threats, programs or applications should only have as much privilege as necessary, requiring the implementation of an explicit security policy that concerns access control, user groups and medical centre staff. However, a policy is only effective if it is adhered to; thus, staff training and education are required to empower the team to understand the necessities of a secure ASMIS. Anderson (2008) indicates that training on effective password management would benefit users, and CAPTCHA can prevent DDoS attempts. Two-factor authentication can also help the verification of patients.

To mitigate social engineering attacks, using soft keyboards help prevent keylogging, password manglers avoid passwords breaches and implement two-channel authentication. Although concerns can be raise as suggested by Anderson (2008) of MITM attacks, which could compromise these methods.

CONCLUSION

The implementation of the ASMIS can stage an excellent opportunity for the medical centre to provide quality service and performance for its patients. The approach in the design must consider the network, software and human factors to standard, guidelines and procedure policy. The policy should include risk assessment for vulnerabilities as seen in the matrix (Mathenge, 2020); where high likeliness levels coincide with high perceived impact, the security administrators should aim to prevent or mitigate threats. Concerning confidentiality, the right users should have the appropriate access levels with encryption used to support data protection. To maintain integrity, there should be effective contingency plans with the trustworthiness of users to promote accountability and responsibility for their conduct. Firewalls such as NGFW should be implemented for reliability and uninterrupted access for users of the ASMIS. Education and training

should be timely and progressive as part of continuing professional development so that medical centre users are aware of the severe threats. This supports prevention mainly where human factors are at high risk and high impact. There is a discussion over implementation costs and whether the expense is justified to provide a secure system. However, with implementation, the effect would be far more severe. Huge financial costs and a higher cost to human life should data breaches occur, or a denial of service could stop emergency medical treatment from being provided.

REFERENCES LIST:

Abrams, L. 2021. *Microsoft fixes Windows Print Spooler PrintNightmare vulnerability* [Online]. Available: https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-print-spooler-printnightmare-vulnerability/#:~:text=In%20June%2C%20a%20security%20researcher,to%20gain%20local%20SYSTEM%20privileges. [Accessed 19 September 2021].

Acronis. N.D. *The NHS cyber attack* [Online]. Available: https://www.acronis.com/en-sg/articles/nhs-cyber-attack/ [Accessed 19 September 2021].

Alhajeri, K. K., Al-Hashimi, M., Badawi, S. & Hamdan, A. 2021. The Impact of the Online Patient Appointment System on the Quality of Health and Medical Services. *In:* HAMDAN, A., HASSANIEN, A. E., KHAMIS, R., ALAREENI, B., RAZZAQUE, A. & AWWAD, B. (eds.) *Applications of Artificial Intelligence in Business, Education and Healthcare.* Cham: Springer International Publishing.

Ambler, S. W. 2005. *The Elements of UML(TM) 2.0 Style*, Cambridge University Press.

Anderson, R. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems,* Indianapolis, USA., Wiley.

Bankole, J. 2019. *MedExpress: Medical Appointment Booking System.* Dublin, National College of Ireland.

Beavers, J. & Pournouri, S. 2019. Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. *Blockchain and Clinical Trial.* Springer.

Brookshear, Brylow & Manasa 2020. *Computer Science: An Overview, eBook, Global Edition.,* London, Pearson.

Center, C. 2015. *Handling Threats from Disgruntled Employees* [Online]. Carnegie Mellon University's Software Engineering Institute. Available: https://insights.sei.cmu.edu/blog/handling-threats-from-disgruntled-employees/ [Accessed 1 October 2021].

Consulting., I. 2019. *General Data Protection Regulation (GDPR) – Official Legal Text* [Online]. Available: https://gdpr-info.eu/ [Accessed 11 August 2021].

Howard, M., Leblanc, D. & Leblanc, D. 2014. *Writing Secure Code : Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World*, Microsoft Press.

Mathenge, J. 2020. *Risk Assessment vs Vulnerability Assessment: How To Use Both* [Online]. Available: https://www.bmc.com/blogs/risk-assessment-vs-vulnerability-assessment/ [Accessed 2 October 2021].

Miller, A. R. & Tucker, C. E. 2011. Encryption and the loss of patient data. *Journal of Policy Analysis and Management,* 30**,** 534-556.

National Cyber Security Centre. 2018. *GDPR security outcomes* [Online]. Available: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes [Accessed 19 September 2021].

Nsrav. N.D. *Denial of Service* [Online]. Open Web Application Security Project. Available: https://owasp.org/www-community/attacks/Denial_of_Service# [Accessed 19 September 2021].

Parmar, V., Large, A., Madden, C. & Das, V. 2009. The online outpatient booking system 'Choose and Book' improves attendance rates at an audiology clinic: a comparative audit. *Journal of Innovation in Health Informatics,* 17**,** 183-186.

Patel, N. 2020. Social engineering as an evolutionary threat to information security in healthcare organisations. *Jurnal Administrasi Kesehatan Indonesia,* 8**,** 56-64.

Sharma, A. 2021. Online Doctor Appointment System.

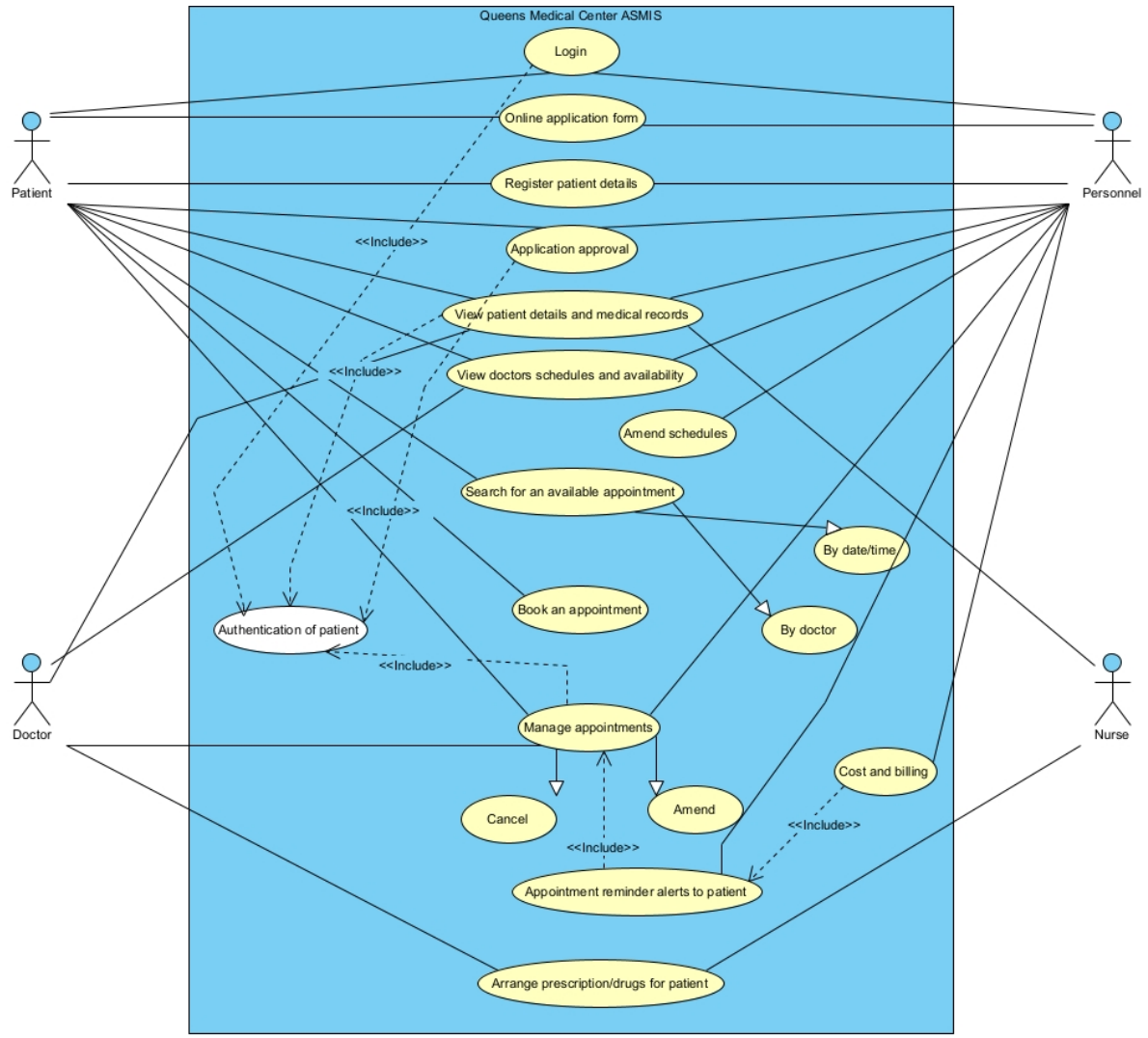
Stine, K. & Dang, Q. 2011. Encryption basics. *Journal of AHIMA,* 82**,** 44-46.

Thomason, S. 2012. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology,* Volume XII.

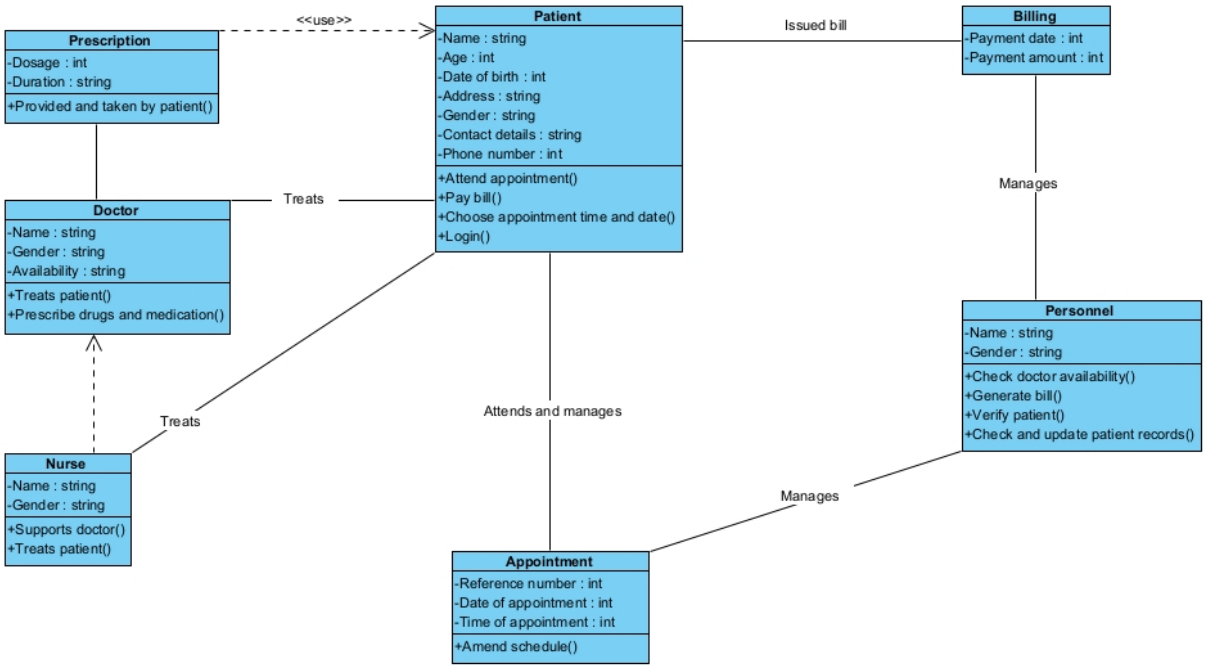
Zarinkhou, S., Nachmias, H., Biderman, O. & Vazgiel, D. 2021. *Demystifying the PrintNightmare Vulnerability* [Online]. Available: https://www.sygnia.co/demystifying-the-printnightmare-vulnerability [Accessed 19 September 2021].

APPENDICES

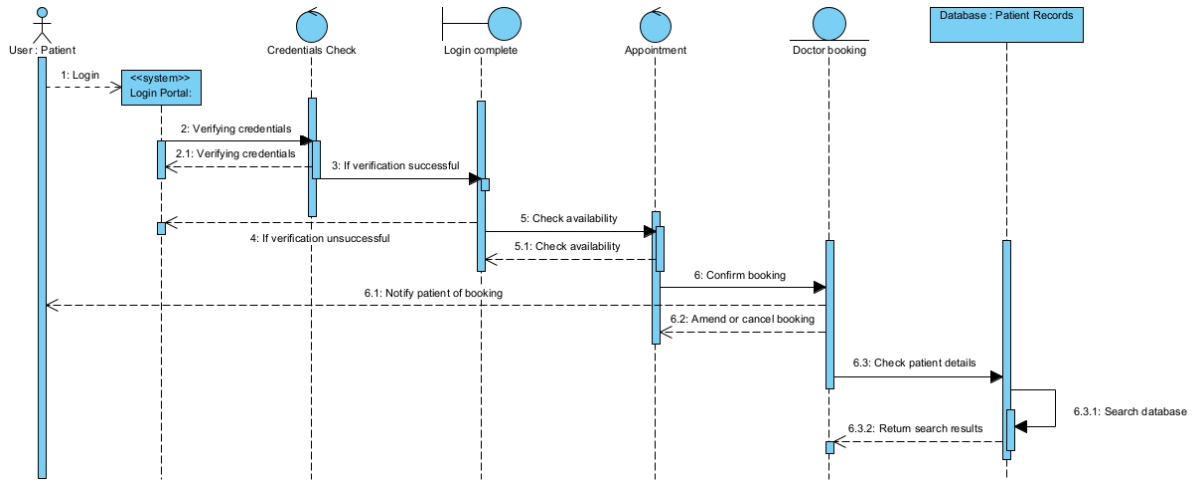
Appendix 1.1 ASMIS behavioural model with inbuilt secured design Use Case Diagram



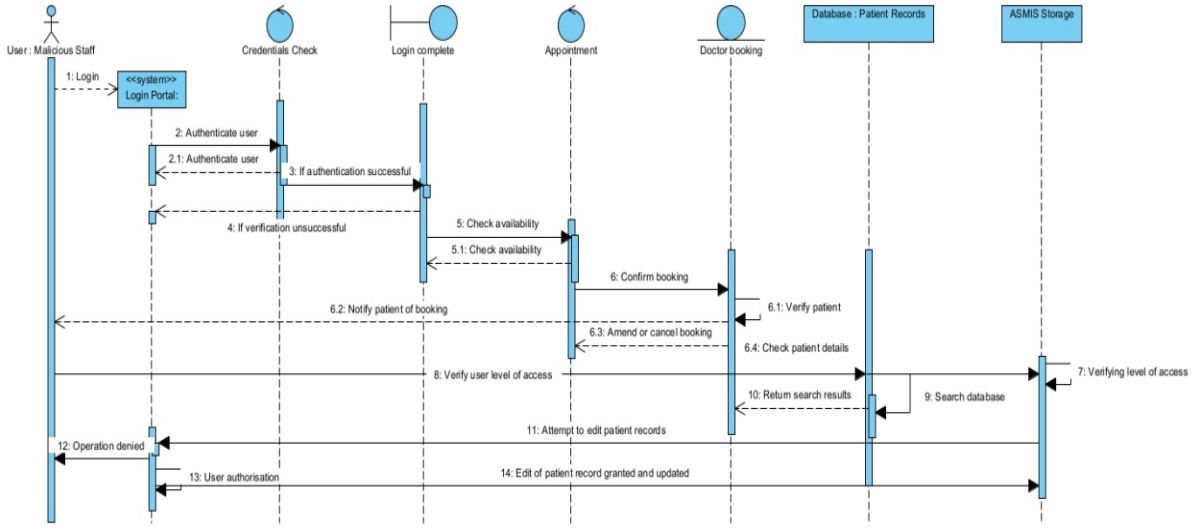
Appendix 1.2 ASMIS structural model with inbuilt secured design Class Diagram



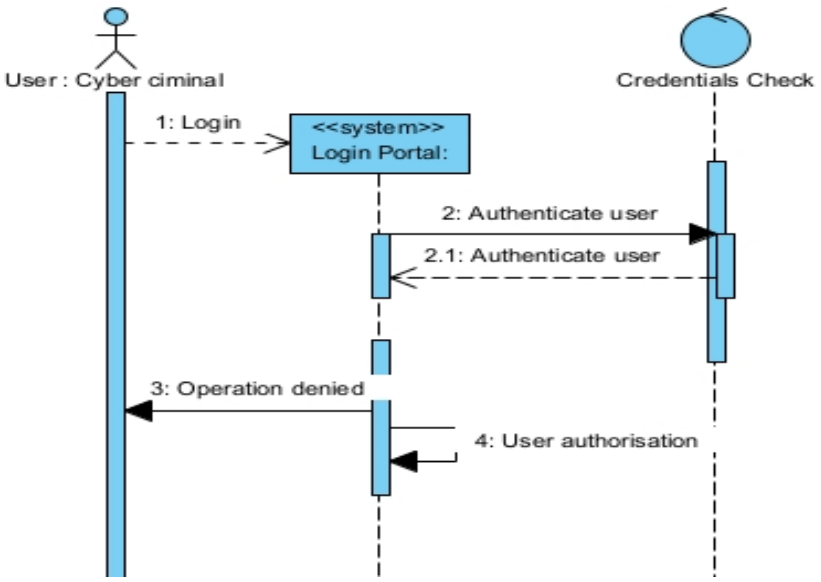
Appendix 1.3 ASMIS behavioural model with inbuilt secured design Sequence Diagram - Patient



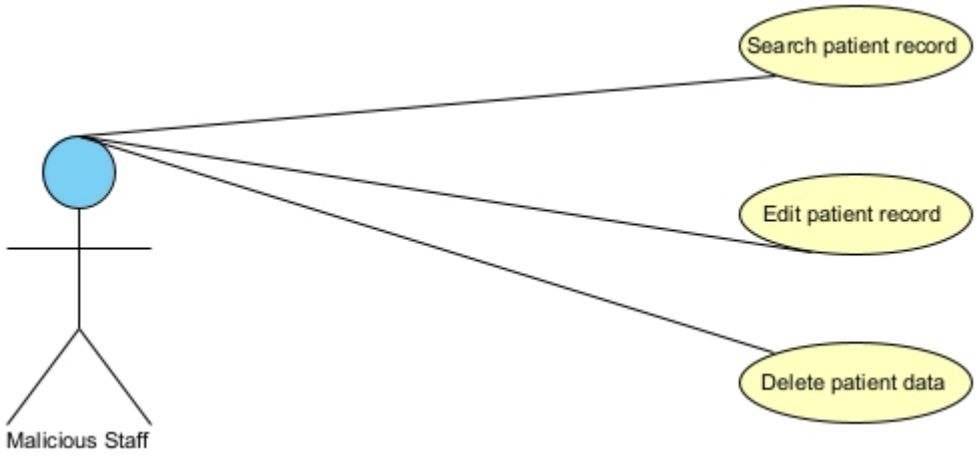
Appendix 2.1 ASMIS behavioural model with inbuilt secured design Sequence Diagram - Malicious Staff



Appendix 2.2 ASMIS behavioural model with inbuilt secured design Sequence Diagram - Cybercriminal



Appendix 2.3 ASMIS Abuse case - Malicious Staff



Appendix 2.4 ASMIS Abuse case - Cybercriminal