ASMIS Cyber Threat Report

by Nomusa Majola

Submission date: 21-Aug-2022 05:33PM (UTC-0400)

Submission ID: 1885108139

File name: 18197_Nomusa_Majola_ASMIS_Cyber_Threat_Report_662549_715263888.docx (483.25K)

Word count: 3933

Character count: 21843

TABLE OF CONTENTS

1. INTRODUCTION..2

2. BENEFITS AND CONSTRAINTS OF ASMIS...4

3. SYSTEM CONFIGURATION 6

4. THREAT MODELLING ANALYSIS AND MITIGATION STRATEGIES...................................10

5. CONCLUSION...20

REFERENCES 21

1. INTRODUCTION

The aim of this report is to identify the cyber security risk and threat inherent with a web-based Appointment and Scheduling Management Information System (ASMIS).

A web-based appointment scheduling system is accessible over the web by patients to make, modify and also manage appointments and patient information. It is also accessible to physicians who can view and confirm appointments. Currently, the only way to make an appointment is via phone or email which is heavily reliant on the receptionist or admin staff managing the diary. This is a major bottleneck given that all appointments have to be made through the receptionist and has the following shortcomings: (a) only one patient appointment can be attended to at a time; (b) booking each patient appointment involves a 5 to 10 minute conversation, and is therefore quite time consuming; (c) appointments can only be made during working hours when the receptionist is at work; and (d) patients have to typically remain on the line for between 20 and 50 minutes to reach the receptionist to make an appointment.

With the advancement of web-based technologies, many medical clinics are shifting to web-based systems that gives the user freedom to make booking in real time and without any working hour restrictions and appointment approval lag experienced with the conventional telephone and email booking system. This effectively addresses all of the challenges mentioned previously and significantly reduces the bottleneck in the appointments booking system.

While they provide these advantages, web-based systems inherently provide remote access to a range of users – both normal and malicious – and are unfortunately potentially exposed to a range of cyber-attacks by cyber criminals. In the case of an ASMIS, the significant risk is the leaking or breaching of patient information, including information about individual consultations, which would be a violation of patient confidentiality.

It is important to note the difference between data breaches and data leaks. Data breaches are the intended outcome of a planned/pre-meditated cyber-attack by cyber criminals, whereas a data leak involves an unintentional pathway, loophole or vulnerability of a system that are unknown to the IT security personnel and have therefore not been patched up. Data leaks result from the exploitation of such vulnerabilities by cyber criminals.

One such data breach for the medical industry was Magellan Health in 2020, where the company became a victim of a sophisticated ransomware attack (Mandal and Khan, 2020). The attack resulted in the breaching of over 300 000 patient records. Malware was used to access employee login information and lodged a phishing attack therefore gaining access to the server. The breached data included personal information of patients. An example of a data leak was the 2021 Microsoft Power leak which was discovered by UpGuard. The leak exposed 38 million Covid vaccination and contact tracing data.

2. BENEFITS AND CONSTRAINTS OF ASMIS

ASMIS allows physicians to manage their booking slots online. Patients can only book empty slots which will be reserved in their name. The ASMIS manages the appointment data for multiple physicians. When a patient visits a doctor, his/her medical entry is stored in the database by the physician. The physician then updates patient consultation notes. This information is recalled from the database every time the physician sees that specific patient.

The benefits of adopting an ASMIS are ;

- Time Saving - The staff spends less time on managing appointments, and phone booking, and can, therefore, use their free time for more urgent and vital tasks. Staff can also attend to special cases such emergencies, having been relieved of dealing with the task of booking general appointments (Zhao et al., 2017) (Cao et al., 2011).
- Money Saving - The time savings made by the facility can translate automatically into monetary savings as a reduction in services and staff translates into a reduction in expenses (Akinode, 2017).
- Convenience – Patients book in real time and are not constrained by working hours. Furthermore, patients need not stay on the line for long periods of time in order to secure a booking (Akinode, 2017) (Cao et al., 2011).
- Centralised information System – Web-based systems make patient management more efficient, since all the information is placed in a centrally located server.
- Scalability – The system is agile enough to be scalable for system requirement changes or technology advancements.

- Increased Efficiency – The use of a web-based system has been noted as in practice as significantly reducing cases of missed appointments by patients (Walters et al., 2003) (Lowes, 2004).

The drawbacks of adopting an ASMIS are:

- It requires complex and extensive calendar synchronisations. While this is not infeasible from an algorithmic and operational point-of-view, it is very likely that exceptional booking scenarios will arise that will not be catered for.
- Its difficult to use for the older demographics who are not technology savvy. These demographics will either have to obtain the assistance of a family member or otherwise resort to the traditional telephonic-based booking system (Cao et al., 2011).
- It is impersonal. A major issue with this is when patients/users enter erroneous data or make erroneous bookings on the system and need assistance to rectify these issues. It is therefore unlikely that an ASMIS can be completely automated, and will rather require at least some human intervention from time to time.
- Accessibility issues during electricity load shedding leading to double bookings and flooding of the telephone lines.

3. SYSTEM CONFIGURATION

Kong et al. (2010) describe UML as being a notation system that can help generate visual models of object-oriented systems. Accordingly, the UML class diagram depicted in **Figure 1** models the objects, requirements and layout of the ASMIS and the specific actions and types of information that will be managed in the system. The diagram also describes the attributes and operations of the classes, their interrelationships and the constraints they might impose on the system.

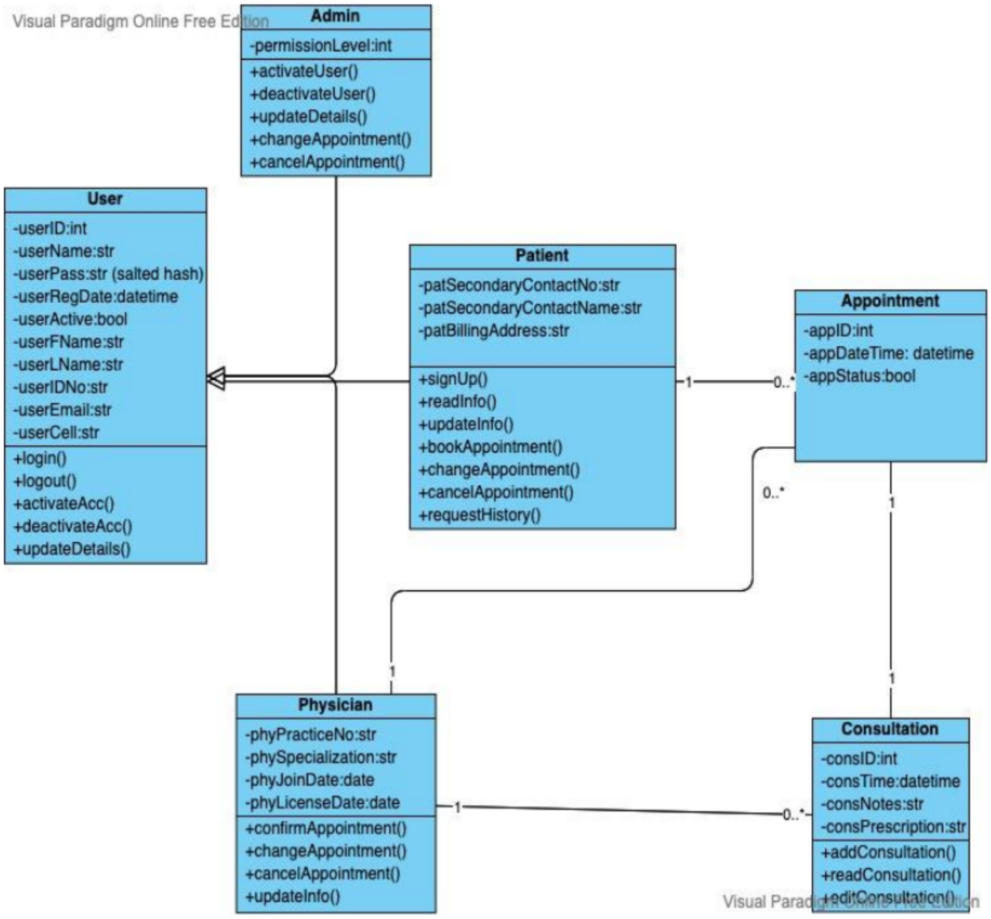

Figure 1:UML class diagram of the proposed ASMIS.

The use case diagrams provided in Figures 2 – 4 below are indicative of the key users of the ASMIS. Use case diagrams help identify various types of users who are going to use the system and the use cases will be often accompanied with various other kind of diagrams as well (Gemino and Parker, 2009).

The patient will open the ASMIS URL and attempt to register themselves and thereafter log and schedule their appointment. Malicious external users normally attempt to brute force the ASMIS and also look for vulnerabilities and loopholes, with the primary objective being the acquirement of access to private and confidential information.

Administrators are provided access and specific privileges to perform their duties. They are able to update and reschedule appointments should the patient not be in a position to do so. Malicious administrators pose the biggest threat as their privilege and level of access allows them to sabotage and abuse or leak confidential information, and this is the area of most concern to the ASMIS from a cyber security point of view.

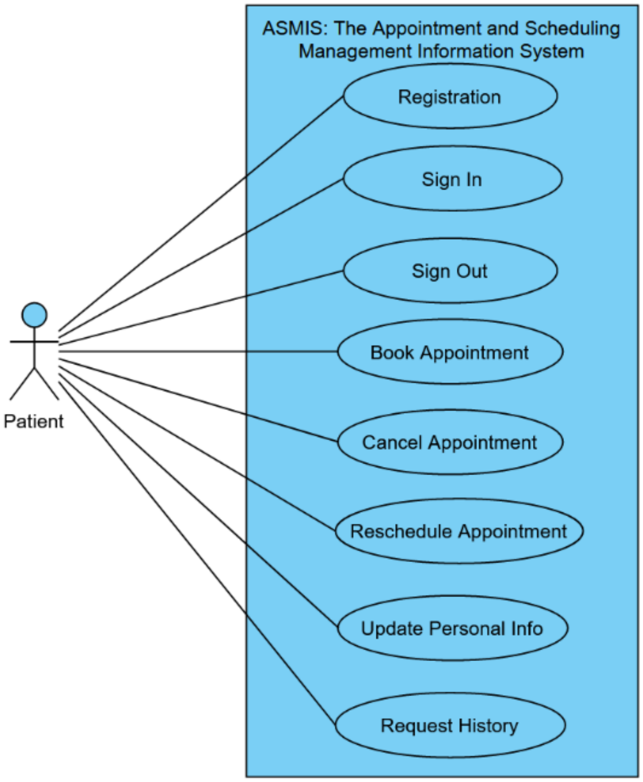

Figure 2: ASMIS use case diagram for a Patient.

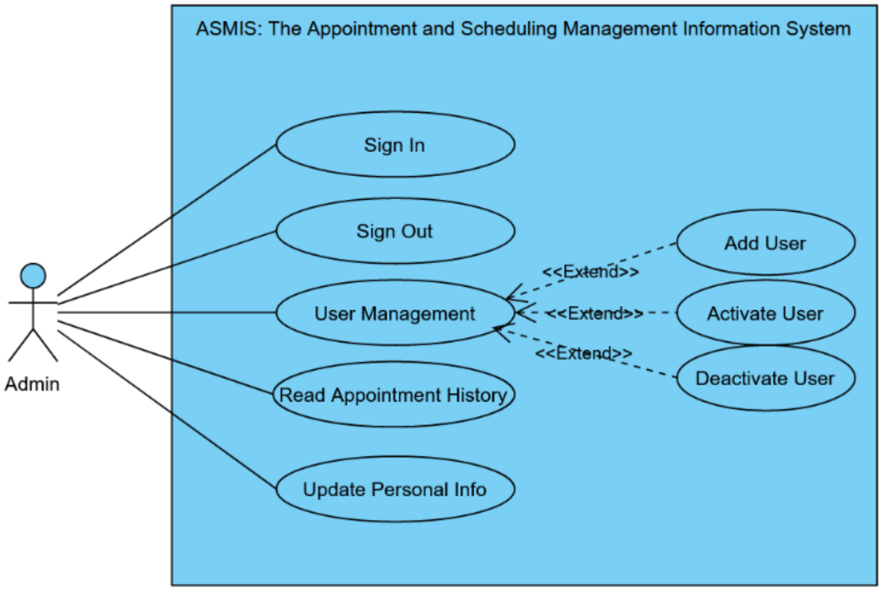

Figure 3: ASMIS use case diagram for an Admin user.

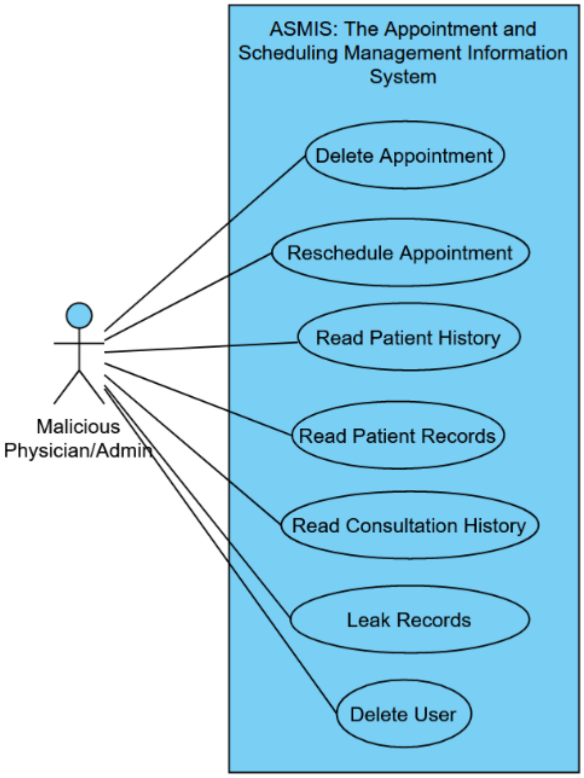
ASMIS: The Appointment and Scheduling Management Information System
Delete Appointment
Reschedule Appointment
Read Patient History
Read Patient Records
Read Consultation History
Leak Records
Delete User
Malicious Physician/Admin

Figure 4: ASMIS use case diagram for a Malicious Physician/Admin user.

4. THREAT MODELLING ANALYSIS AND MITIGATION STRATEGIES

This section provides a detailed analysis of various security threats to the ASMIS as well as providing recommendations on measures that can effectively mitigate these threats.

The core reason for threat modeling is to correctly define critical use cases that are capable of delivering cybersecurity and privacy risk assessments on ASMIS (Steven, 2010). For the purposes of this report, the threat modelling method used to assess and mitigate the security risks to the proposed ASMIS is a combination of an attack tree (Lallie et al., 2020) and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) threat analysis (Khan et al., 2017).

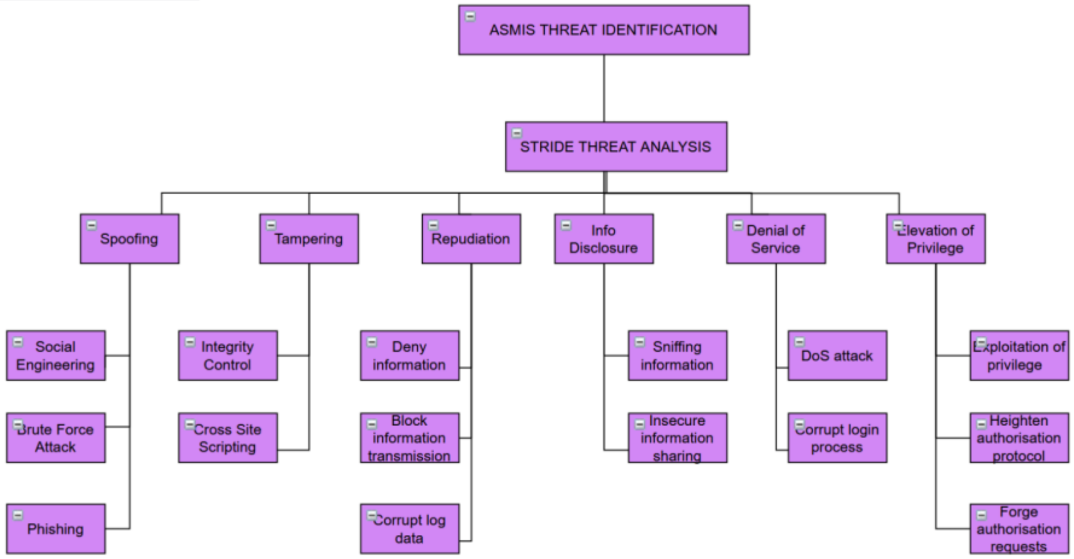

Figure 5: ASMIS attack-tree analysis.

The attack-tree depicted in Figure 5 offers a detailed and highly structured visualization of the strengths and weaknesses of the ASMIS system. Using a combination of this attack-tree and STRIDE analysis has enabled for better visualization of the identified security services and features and this paves the way for building more robust and secure systems. STRIDE analysis aims to identify threats in specific threat categories, namely, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (Khan et al., 2017).

Table **1** summarizes all of the STRIDE threats, along with explanations and examples of scenarios in which those threats may be realized / actuated.

Table 1: ASMIS STRIDE threat analysis

Property	Threat	Definition	Example
Authentication	**S**poofing	Impersonating something or someone else.	Pretending to be any of the role players. i.e. doctor, administrator ,patient. Brute forcing, Phishing, social engineering
Integrity	**T**ampering	Modifying data or code	Modifying patient or doctor information. Modifying the clinic patient database. Modifying unencrypted data in transit. Modifying ASMIS framework code.
Non-repudiation	**R**epudiation	Claiming to have not performed an action.	Removal of event and activity logs to destroy evidence trails leading to perpetrators of malicious activity.
Confidentiality	**I**nformation Disclosure	Exposing information to someone not authorized to see it	Exposing sensitive information to unauthorized users e.g. displaying patient personal or consultation information due to ASMIS code errors, interception

Property	Threat	Definition	Example
			of unencrypted data in transit or in the database.
Availability	**D**enial of Service	Deny or degrade service to users	Flooding the ASMIS with illegitimate simulated requests, consuming and overworking the server CPU, and making the ASMIS unusably slow or even unresponsive.
Authorization	**E**levation of Privilege	Gain capabilities without proper authorization	Allowing a remote unauthorised user to run commands on the system OS or database like amending patient records. Patient getting privileges or full access usually only accessible to a privileged admin user.

With reference to

Table **1**, the threats of concern along with mitigating solutions are described below:

Spoofing:

Spoofing allows a user to impersonate another user, thereby obtaining unsolicited access to a system, and gaining access to potentially sensitive data that they might not ordinarily have access to.

Threat: One form of spoofing attacks involve hackers making use of attacks such as phishing and pretexting attacks. Phishing attacks involve the attacker sending seemingly genuine emails or at times carrying out phone calls on behalf of the organization to key system users, thereby deceiving these users to disclose their credentials (Gupta et al., 2016). Phishing attacks are the most common type of social engineering attack, occurring either verbally or electronically. Pretexting attacks are very similar to phishing attacks and have the same goal, but differ in that the attacker in this case aims to deceive the user that he/she requires key information to authenticate them.

Mitigation: IT security personnel should regularly educate staff at all levels, but especially users with elevated access rights, on the realities of these kinds of attacks. This can involve email and video communications, but also scheduled workshops. The human aspect of the organization has been noted as being a major source of vulnerability in an ASMIS-type system (Tsochev et al., 2020). Carrying out regular simulated phishing and pre-texting attacks on users within the organization to assess and address weak links can also help mitigate this threat. Various third-party software installed on internal client devices such as firewalls, anti-malware and anti-virus software can help filter out email and software-based phishing attacks to a large extent. Such software should be updated regularly in order to ensure that up-to-date protection is provided.

Threat: Another form of spoofing involves the attackers using social engineering techniques to gain physical access to the server(s) hosting the ASMIS. The attacker will typically pose as an employee or maintenance personnel, thereby circumventing any physical access control policies.

Mitigation: Educational activities and controlled drills will also help mitigate this threat. Furthermore, instituting strict access control and logging policies, including access cards and biometric access along with video monitoring, over the server room will help mitigate this threat.

Threat: Spoofing attacks may also take the form of dictionary / brute force attacks which involve the use of software automation tools to attempt multiple username and password combinations until a match is achieved, and unsolicited access is obtained.
Mitigation: A combination of captcha when logging in, coupled with a strict password policy (e.g. minimum of 10 characters, at least one special, upper-case and lower-case character, and at least one digit) and a login delay policy (e.g. increasing periods of time between successive failed login attempts after a given minimum of three tries) for unsuccessful login attempts can help mitigate this threat.

Tampering:

Tampering speaks to the modification and manipulation of exposed data or code. This can affect the underlying code of the ASMIS itself, the operations of the ASMIS and/or the data moved around by the ASMIS as it operates (De Souza et al., 2020).

Threat: Web-based frameworks are developed with security in mind, but bugs and unknown vulnerabilities in this code are an accepted fact of life. These bugs and vulnerabilities are known as exploits since, once they are known to attackers, can be exploited to circumvent and gain potentially complete access to the system.
Mitigation: The IT team must schedule regular updates to the underlying ASMIS framework, including the database management software (DBMS) and server software to ensure that all known security vulnerabilities have been patched.

Threat: Another class of tampering attacks are code-injection techniques such as cross-site scripting (XSS or CSS) and SQL injection attacks. In these cases, attackers capitalize on insecure user input policies to inject malicious code into the server, thereby, running commands, stealing information and impersonating other users.

Mitigation: The ASMIS acquired must be built on top of a reputable secure framework, as such frameworks will automatically include measures/code that sanitizes all user input in the ASMIS to prevent XSS or SQL injection attacks.

Threat: Tampering may also involve the interception and modification of insecure data in transit, thereby obtaining sensitive information such as credentials, and/or gaining access.

Mitigation: TLS should be implemented on the ASMIS server to consistently encrypt all messages sent to and from the ASMIS server. Care must be taken when doing so as an incorrect configuration of TLS will have compromised security e.g. using an obsolete version.

Repudiation:

Threat: This is when threat events and activity logs are erased in order to destroy evidence trails leading to perpetrators (Khan et al., 2017) (Shevchenko et al., 2018). In so doing, the ASMIS may not have any record of having received information from a client, or a client may not have record of having received information from the ASMIS. Repudiation makes it difficult or even impossible to track the source of a threat, thereby creating a more inviting environment of anonymity for potential attackers.

Mitigation: Activity logs and the entire system database should be regularly backed up on one or more external sites. Furthermore, encrypting the logs and the database can help prevent these items being changed to mislead investigators or hide evidence.

Logs should be protected behind appropriate user access controls and remote access to such logs should be prevented in this way.

Information Disclosure (ID):

ID involves exposing sensitive information to unauthorized users (Honkaranta et al., 2021).

Threat: This could involve the displaying of sensitive information such as patient, appointment, consultation or user information as a result of errors in the underlying code, or weak security policies on the ASMIS server.

Mitigation: Regular patches to the ASMIS framework, database and server software. Furthermore, access controls on the ASMIS server must be carefully setup to prevent unsolicited access.

Threat: Weak or absent encryption on the data as it is transmitted from the ASMIS to clients can be intercepted via packet sniffing. This can provide attackers access to various types of sensitive data while it is in transit.

Mitigation: This can also be addressed by means of TLS encryption on the ASMIS server.

Threat: Attacks on the underlying DBMS using known exploits may provide access to the ASMIS database and if the data in the database in unencrypted, this will constitute information disclosure.

Mitigation: Regular updates to the DBMS must be scheduled. Also, the data in the database must be encrypted; in the event that a breach or leak of the database takes place, encrypted data will be of much less risk than if it were in raw unencrypted form.

Threat: Providing the ability for users to access unnecessarily large volumes of sensitive information outside of their context of use and without any additional authentication and/or logging measures can make the system susceptible to abuse e.g. an admin user having the ability to access many/all patient/consultation records at a time, without any further authentication and moreover in the absence of logging.

Mitigation: Sensitive actions by potentially malicious user roles such as the admin role should be limited to accessing a small number or even one record at a time within context. Multi-factor authentication can be used to obtain consent by an affected patient every time that their (personal or consultation) data is accessed. This can take the form of a one-time pin. Furthermore, extensive logging of all activities carried out on the system, e.g. creation, modification and cancellation of appointments and searching and updating of patient or consultation records, can foster an environment of responsible access and use; malicious users will be reluctant to engage in malicious activity in the absence of anonymity.

Denial of Service (DoS):

Threat: This involves overloading the ASMIS server by flooding the system with simulated traffic to consume its processors and prevent processing of legitimate actions (Chao-Yang, 2011). This can cause the ASMIS to appear to be very slow or, in the extreme case, offline to legitimate users. DoS attacks can provide attackers with information such as response times and routing information. DoS attacks may also be used as a distraction by attackers while attempting other forms of attacks on the ASMIS.

Mitigation: The use of Next-Generation Firewalls (NGFWs) such as Checkpoint and Fortinet, among others, have in-built DoS (including distributed DoS) attack prevention capabilities, and can effectively detect and filter malicious DoS traffic from the ASMIS server. The use of such NGFWs is an absolute necessity for the ASMIS.

Elevation of privilege (EoP):

This entails a hacker obtaining access to activities that are normally only accessible to key high-level (i.e. privileged) users such as high-level administrators (Li et al., 2016). In so doing, the hacker is able to get access to sensitive information and carry out malicious actions on the system.

Threat: EoP can be obtained by a skilled hacker experimenting with the ASMIS operational logic and discovering loopholes / flaws in the operational logic that provide elevated rights to common users. It could also involve attackers making use of known exploits in the underlying ASMIS framework, database or server software / operating system to gain EoP rights.

Mitigation: Applying regular scheduled software updates to the underlying ASMIS framework and DBMS software can help remove many such operational logic loopholes which are regularly uncovered and patched. Furthermore, regular penetration tests can be scheduled to uncover further loopholes which can then be addressed as they come up.

Threat: It can also involve an attacker gaining access to a logged-in system of a privileged user in the absence of an appropriate timeout / lock-out policy while the privileged user is not at his/her desk e.g. an administrator at the clinic.

Mitigation: Including the use of access cards for sensitive high-level users, which access cards would be carried by the users in question e.g. worn around their necks. When logging in, such users would have to insert their access card, and as soon as they leave their workstation, the access card is automatically removed, thereby logging the user out of the workstation.

Figure 6 below depicts a sequence diagram that demonstrates specific activities that a malicious admin may carry out to compromise the ASMIS system or data, as well as various controls that can mitigate/prevent the damage done by these actions.

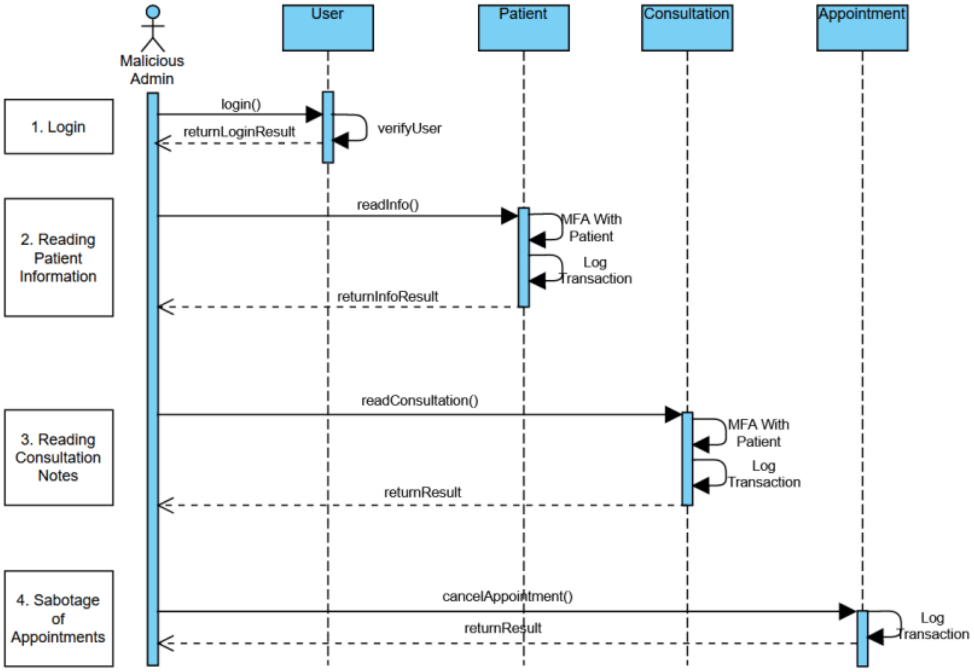

Figure 6: ASMIS use case for a malicious admin user.

5. CONCLUSION

There are various cyber security solutions available for securing and increasing defences within an ASMIS. Due to the web environment being overly agile, it becomes a constant marathon to remain ahead of security threats. Incorporating multi-disciplinary strategies is vital . System violations have significant consequences for the clinic not only for delivering efficient services, but legal, financial and reputational related implications. Inefficient ASMIS security may not be able to prevent all cyber-threats which may destabilize the clinic system or lead to the loss of control or loss of comfort during users' sessions. It is vital for all security measures to provide multi-layered defence and regularly audit user safety and update security mechanisms and protocols.

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.

Cao, W., Wan, Y., Tu, H., Shang, F., Liu, D., Tan, Z., Sun, C., Ye, Q. and Xu, Y., 2011. A web-based appointment system to reduce waiting for outpatients: A retrospective study. BMC health services research, 11(1), pp.1-5.

Chao-Yang, Z., 2011, August. DOS attack analysis and study of new measures to prevent. In 2011 International Conference on Intelligence Science and Information Engineering (pp. 426-429). IEEE.

De Souza, N.P., César, C.D.A.C., de Melo Bezerra, J. and Hirata, C.M., 2020. Extending STPA with STRIDE to identify cybersecurity loss scenarios. Journal of Information Security and Applications, 55, p.102620.

Gemino, A. and Parker, D., 2009. Use case diagrams in support of use case modeling: Deriving understanding from the picture. Journal of Database Management (JDM), 20(1), pp.1-24.

Gupta, S., Singhal, A. and Kapoor, A., 2016, April. A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.

Honkaranta, A., Leppänen, T. and Costin, A., 2021, May. Towards practical cybersecurity mapping of stride and cwe—a multi-perspective approach. In 2021 29th Conference of Open Innovations Association (FRUCT) (pp. 150-159). IEEE.

Khan, R., McLaughlin, K., Laverty, D. and Sezer, S., 2017, September. STRIDE-based threat modeling for cyber-physical systems. In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe) (pp. 1-6). IEEE.

Lallie, H.S., Debattista, K. and Bal, J., 2020. A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review, 35, p.100219.

Li, M., Huang, W., Wang, Y., Fan, W. and Li, J., 2016, June. The study of APT attack stage model. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) (pp. 1-5). IEEE.

Lowes R. (2004) Phones driving you crazy? Try clinical messaging. *National Library of Medicine,* 81(6): 65-76.

Mandal, S. and Khan, D.A., 2020, September. A Study of security threats in cloud: Passive impact of COVID-19 pandemic. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 837-842). IEEE.

Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P. and Woody, C., 2018. Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Steven, J., 2010. Threat modeling-perhaps it's time. IEEE Security & Privacy, 8(3), pp.83-86.

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S. and Pavlova, G., 2020, October. Cyber security: Threats and Challenges. In 2020 International Conference Automatics and Informatics (ICAI) (pp. 1-6). IEEE.

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.

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.

ASMIS Cyber Threat Report

ORIGINALITY REPORT

19%	16%	7%	17%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Kaplan College Student Paper	3%
2	Submitted to University of Wales Institute, Cardiff Student Paper	2%
3	mocdoc.in Internet Source	1%
4	Submitted to Roehampton University Student Paper	1%
5	Duszan Augustyn, Andrea Tick. "Security Threats in Online Metasearch Booking Services", 2020 IEEE 20th International Symposium on Computational Intelligence and Informatics (CINTI), 2020 Publication	1%
6	Submitted to London School of Commerce Student Paper	1%
7	Submitted to Nelson Mandela Metropolitan University Student Paper	1%

8	Submitted to University of Warwick Student Paper	1 %
9	Submitted to Glyndwr University Student Paper	1 %
10	www.routledge.com Internet Source	1 %
11	Submitted to University of Gloucestershire Student Paper	1 %
12	Submitted to The University of the West of Scotland Student Paper	1 %
13	Submitted to Purdue University Student Paper	1 %
14	Submitted to Webster University Student Paper	1 %
15	Submitted to University of Wolverhampton Student Paper	1 %
16	www.slideshare.net Internet Source	1 %
17	Submitted to Heriot-Watt University Student Paper	1 %
18	www.upguard.com Internet Source	1 %
19	Submitted to University of Liverpool	

	Student Paper	<1 %
20	pure.port.ac.uk Internet Source	<1 %
21	Submitted to University of Northumbria at Newcastle Student Paper	<1 %
22	cris.vtt.fi Internet Source	<1 %
23	ebin.pub Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		