**Introduction**

In hospitals and other care facilities, appointment and scheduling management information systems (ASMIS) are widely regarded as the most effective tools for solving the challenges of long wait times. The systems allow for patients to schedule appointments with care providers before they arrive at the hospital. This helps to significantly enhance the patient experience by minimizing wait times and improving the facility's operational efficiency. Most ASMIS systems are built on a 5-step operational model; the steps are:

1. Appointment booking- the patient is able to book an appointment at the care facility specifying the type of care he/she will be seeking to allow the system to match him/her with the appropriate specialist.
2. Reminder Notifications- the patients receive a notification reminding him/her of the appointment a few days or hours to the scheduled date.
3. Self-check-in- the patients are able to check-in by themselves using links embedded in the notification message.
4. Automated ticketing- the p atient receives an automated ticket after check-in which informs them of the specialist they will consult and the room number.
5. Consultation notification- Patient receives a notification when it is time to receive the service (Qaffas, and Barker, 2011).

**Benefits of ASMIS**

**Reduced Wait Time**

The ASMIS systems offer a number of benefits that can improve the operational efficiency of Queens medical center. One of the primary advantages of ASMIS is that they help to significantly reduce wait time for care facilities (Zhao et al., 2017). The system staggers patients' appointments at different times of the day and this reduces the risk of multiple patients arriving for a consultation at the same time. By eliminating the risk of patient overcrowding, the system automatically reduces the wait times and this, in turn, helps to improve patient experiences.

**Creates a Happier Working Environment**

Care providers hold that the ASMIS systems help to significantly improve their working environment. By staggering patients' appointments to different times of the day, the system helps to manage the workload on care providers. The distribution of workload at different times of the day to reduce stress and anxiety among the care providers, making the working environment more accommodating (Zhao et al., 2017). It also enables care providers to serve more patients as they are more relaxed and organizes.

**Improves operational and staff efficiency**

The use of ASMIS helps to improve both operational and staff efficiency at the hospital. Operational efficiency is improved by eliminating the manual appointment routine, freeing up staff to work in other areas of the facility (Zhao et al., 2017). Staff efficiency is improved by managing their workload, allowing optimal performance.

**Better follow-up**

Another major advantage of ASMIS is that it allows better patient follow-up, because information relating to the patient is effectively captured through automated mediums and hence they can be prompted through notifications for return visits or follow-up requests. The systems provide an efficient mechanism through which the care facility can be able to communicate with the patients.

**Challenges with ASMIS**

**Reduced availability for Urgent Cases**

One of the major challenges of ASMIS systems is that they reduce their level of availability to handle urgent cases. The systems are usually not designed to account for urgent cases and as a result of this, the care providers are usually not available to respond to urgent cases that might arise in the facility (Gupta, and Denton, 2008). This is a major challenge as care providers usually need to be pulled out of their appointments to respond to urgent cases (Gupta, and Denton, 2008). As a result, the system gets plagued with a scheduling backlog and the appointments have to be rescheduled.

**Locks-out different segments of the society**

Another major challenge of the ASMIS system is that it locks out a specific segment of society from receiving health care. The systems exclude tech-illiterate individuals as they might not have the skills needed to effectively make appointments (Gupta, and Denton, 2008). The systems also exclude individuals who might not have access to the resources needed to make the appointments (Gupta, and Denton, 2008). For example, those without access to the internet or phones are not able to make appointments.

**Cyber Threats**

**Distributed Denial of Service Attacks**

One of the common forms of cyber-attacks against health institutions is DDOS attacks. The attacks entail overloading a system with requests and causing it to crash as it cannot effectively handle the volume of requests (Humayun et al., 2020). The scheduling systems are prone to DDOS attacks because they are patients driven. Attackers create multiple dummy accounts and use them to overload the system with requests causing it to crash (Humayun et al., 2020). This results in the system being unavailable for those patients who legitimately need to use it to schedule their appointments.

**Phishing Attacks**

Another potential cyber threat facing ASMIS systems is phishing attacks. Over the years there has been a drastic increase in cases of phishing attacks targeted against patients (Humayun et al., 2020). Attackers posing as representatives of the care facilities push corrupted notifications to patients. The attackers convince the patients to login into phishing pages which makes it possible for the attackers to access the patient’s personal information (Abomhara, and Køien, 2015). Phishing attacks against the hospital can also result in attackers obtaining access to the patient’s personal records.

**Third-party attacks**

Another major cyber threat against ASMIS is third-party attackers. The scheduling applications usually store patients' data on mobile devices. Third-party applications are able to access the data by exploiting permission guidelines for the device (Humayun et al., 2020). This is a major issue as it results in the exposure of the patient’s private data.

**Ransomware attacks**

Over the past couple of years, care facilities have increasingly been targeted by ransomware attackers. Studies have demonstrated that Ransomware attacks usually target resources that are of critical importance to the organization (Humayun et al., 2020). Based on this it is logical for one to argue that the ASMIS system provides a new vector through which a ransomware attack can be executed against. This is because it stores sensitive patient data and the hospital is reliant on it for its operations. By attacking the system, the attackers can cripple the hospitals' operations as patients will no longer be able to make appointments and care providers cannot plan their day.

**Use Case UML Diagram**

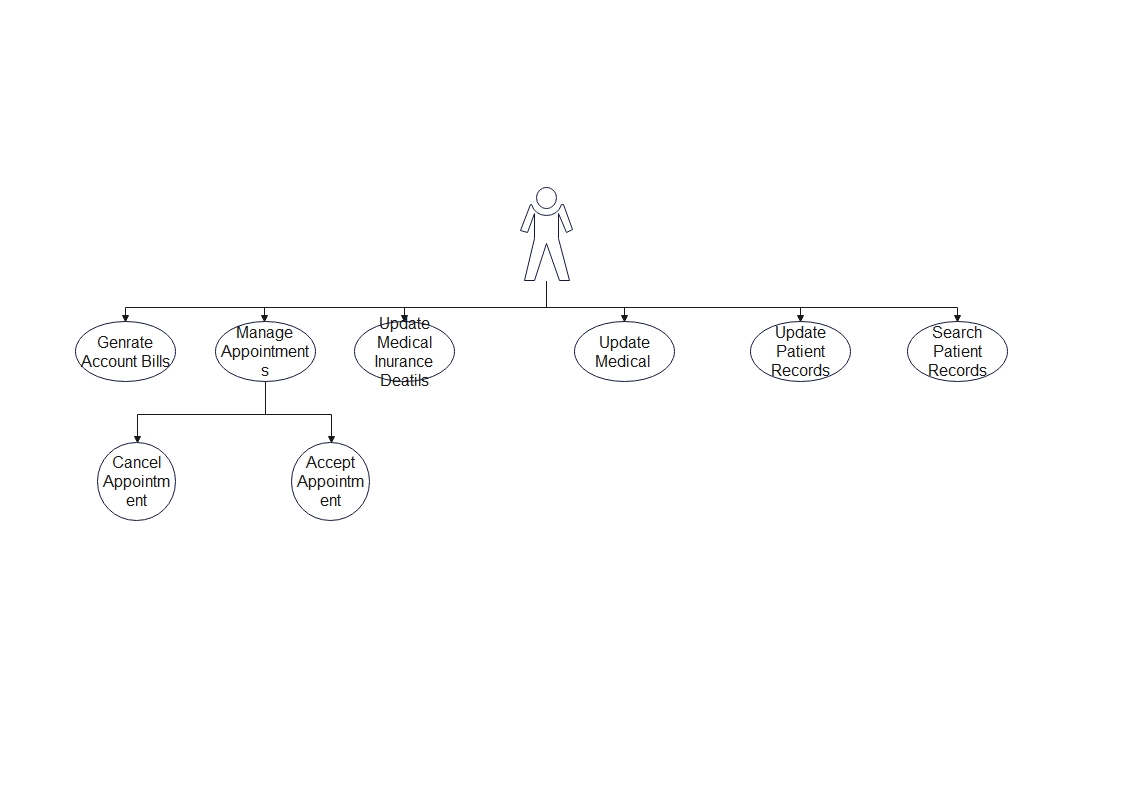
****

Figure 1: non-malicious user - Use Case (ASMIS)

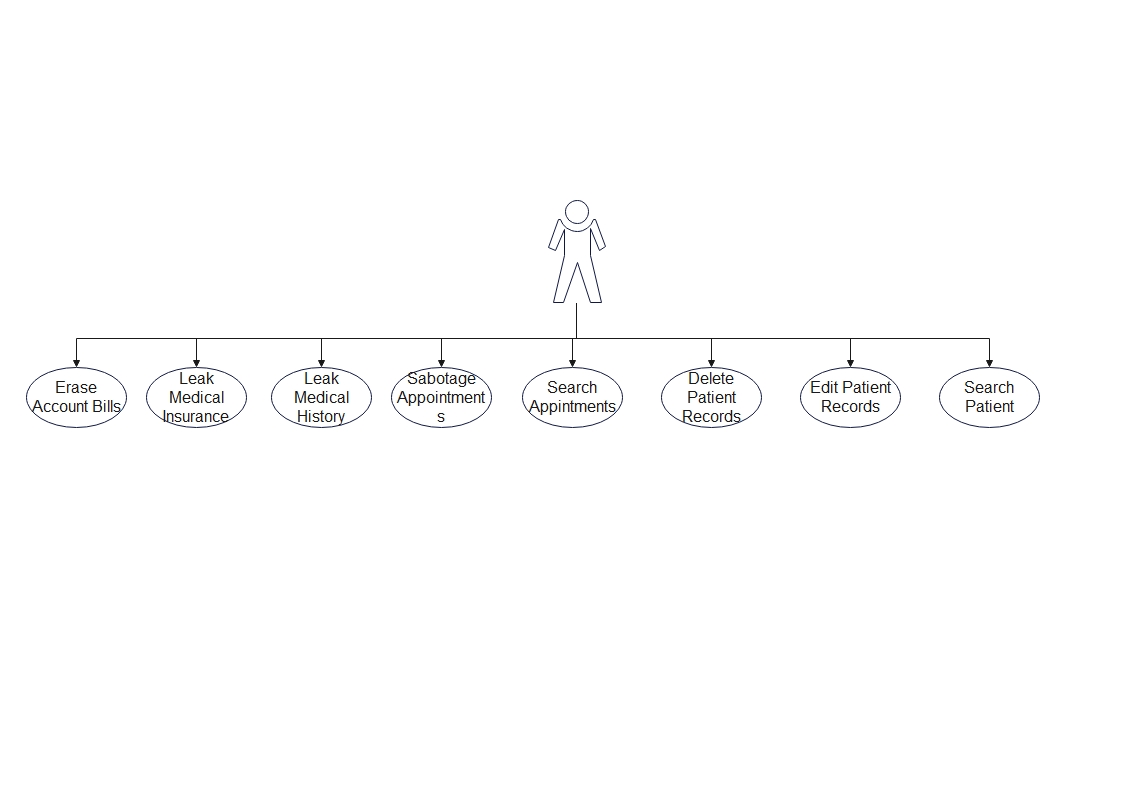


Figure 2: Malicious User - Abuse Case (ASMIS)

The use case UML diagram is the most popular form of behavioral UML diagram. The diagram provides a graphical overview of the different actors who are involved in a system, the functions that are needed by the actors, and the interaction that exists between the different functions. The use case UML makes it easy for one to identify all the primary actors and processes of a system. The diagram graphically represents a system’s workflow describing the operational workflow of the ASMIS thereby making it easy for one to understand how the system functions making it logical that the most effective threat modeling technique that the organization can implement is STRIDE threat modeling.

**STRIDE**

STRIDE is a model that is used in the identification of threats to a computer system (Khan et al., 2017). The model was developed by Microsoft Engineers Loren Kohnfelder and Praerit Garg in the late 1990s as a tool for evaluating systems to identify all potential threats (Khan et al., 2017). The STRIDE model divides threats into six main categories namely spoofing, tampering, repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The model aims at ensuring that the system meets all CIA (Confidentiality, Integrity, and availability) requirements (Khan et al., 2017). This is especially important for hospitals given that the CIA requirements are in line with HIPPA guidelines on data management.

Spoofing occurs when an attacker or program pretends to be another (Khan et al., 2017). An example of this is seen in phishing attacks when attackers send notifications to patients pretending to be hospital representatives. It is also seen when attackers create fake clone websites/applications of the hospital ASMIS. Through spoofing, attackers are able to access sensitive information from the targeted party. Tampering refers to the practices of modifying code or components (Abomhara et al., 2015). Evidence of tampering can be seen when attackers alter the ASMIS code to create clone websites that allow them to acquire sensitive data from the patients and hospital staff. Repudiation refers to threats that are not monitored or logged thereby making it difficult for users to identify them (Abomhara et al., 2015).

Information disclosure refers to a situation in which sensitive data is leaked to unauthorized personnel. In the hospital, information disclosure occurs when attackers are able to access patient health records. This is a major issue as it is a violation of HIPPA regulations and places the patient’s safety at risk. Denial of service refers to a situation in which services or elements of the systems are overloaded with requests leading to a slowdown of operations and in some instances preventing legitimate use (Abomhara et al., 2015). Denial of service attacks can be executed when attackers spam the sign-up page with multiple requests causing the system to crash. Privilege escalation occurs when attackers access the system and grant themselves additional privileges to allow them to obtain greater control over the system (Abomhara et al., 2015). This form of attack is usually performed by personnel who are within the organization and looking to enhance their level of control without seeking the relevant approval.

**Cyber Security Technologies to Mitigate the Threat**

**SSL Certification**

One of the most effective strategies for mitigating the threat of phishing (spoofing) is the incorporation of Secure Socket Layer (SSL) certification to the website. SSL certificates are digital certificates that are employed in the authentication of the identity of a website and facilitating encryption (Sayal et al., 2020). The term secure socket layer refers to a security protocol establishes encrypted links between a web browser and a web server (Sayal et al., 2020). SSL certificates help to secure online transactions and facilitate the privacy and security of user information. The certification encrypts data from the user making it impossible for attackers to read and alter the data. It ensures the security of the connection through an SSL handshake. The handshake is where the web server sends a copy of the certificate to the browser which evaluates its authenticity (Sayal et al., 2020). Once the certificate is deemed to be authentic, the browser prompts the webserver to create a secure communication channel that would facilitate the exchange of data between the two. Users are able to easily tell if a site has SSL certification or not by looking at the URL tab. Sites with SSL certification usually have a padlock sign while those without do not (Sayal et al., 2020). Enabling SSL certification would help the hospital in significantly mitigating the risk of phishing attacks through secure authentication.

An example of SSL certification can be seen with the PayPal site and almost all other legitimate sites on the internet. The main strength of SSL certificates is that they help to significantly increase the security of websites through data encryption and user authentication. Another major advantage of SSL certificates is that it does not require the client to install any software making them easy to implement. Lastly, sites that are SSL secured rank better than those that are not in Google searches. The main weakness of SSL certification is that it reduces the speed of the website's transaction thereby negatively impacting its performance (Sayal et al., 2020). However, it is important to note that the reduced performance is only notable for sites with a large number of visitors.

**Multi-Factor Authentication**

Another technological advancement that can be used to mitigate the threat of phishing is the application of multi-factor authentication (MFA). Multi-factor authentication refers to an authentication method in which a user is granted access to an application or a website only after successfully providing two or more forms of evidence that would help identify his/her identity (Ometov et al., 2018). Most multi-factor authentication systems utilize unique one-time codes which are sent to the user via phone or email. the user is then required to input the codes into the website/application to authenticate their identity (Ometov et al., 2018). The use of MFA helps to ensure that even if an attacker is able to successfully obtain the login credentials (username and password) they still won’t be able to access the site because they won't be able to acquire the authentication code (Ometov et al., 2018). This helps to ensure the security of the user’s account and keep track of his logins thereby mitigating the risk of repudiation.

The use of MFA helps to prevent unauthorized access to a system, protecting the user data and enhancing the security of the system (Ometov et al., 2018). An example of multi-factor authentication can be seen in the Google website which requires multifactor authentication for a user to log into Google accounts. The main strength of MFA is that it enhances security and ensures compliance with a number of regulatory requirements on data privacy (Ometov et al., 2018). The main weakness of MFA is that it is costly to implement there exists a number of technological gaps with regards to MFA implementation.

**Web Application Firewalls and CDNs**

Another solution is the adoption of Web Application Firewalls (WAF) and Content Distribution Network (CDN). The WAF helps to enhance web security by monitoring and filtering all HTTP traffic between the internet and the web application (Dermann et al., 2008). It is able to protect the website from common forms of cyber-attacks like cross-site scripting, cross-site forgery, SQL injection, and file inclusion (Dermann et al., 2008). The CDN on the other hand mitigates the risk of a DOS attack by balancing out website traffic across multiple servers in different locations (Dermann et al., 2008). This helps to reduce the workload on a single server, mitigating the risk of server overload. Evidence of WAF and CDN can be seen in platforms like Netflix and Amazon where traffic is balanced across multiple servers in different regions. The main strength of WFA and CDN is that they help to ensure website integrity and continuity by shielding it from attacks. The main weakness is that they are only effective against a particular type of attack and can be breached by attacks outside their scope.

**Reference List:**

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B.J. and Simoes, E., 2017. Web-based medical appointment systems: A systematic review. Journal of medical Internet research, 19(4), p.e134.

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.

Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45(4), pp.3171-3189.

Gupta, D. and Denton, B., 2008. Appointment scheduling in health care: Challenges and opportunities. IIE transactions, 40(9), pp.800-819.

Abomhara, M. and Køien, G.M., 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, pp.65-88.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-factor authentication: A survey. Cryptography, 2(1), p.1.

Sayal, M.A., Alameady, M.H. and Albermany, S.A., 2020. The Use of SSL and TLS Protocols in Providing a Secure Environment for e-commerce Sites. Webology, 17(2).

Abomhara, M., Gerdes, M. and Køien, G.M., 2015. A stride-based threat model for telehealth systems. Norsk informasjonssikkerhetskonferanse (NISK), 8(1), pp.82-96.

Qaffas, A. and Barker, T., 2011. Online Appointment Management System. In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Dermann, M., Dziadzka, M., Hemkemeier, B., Hoffmann, A., Meisel, A., Rohr, M. and Schreiber, T., 2008. Best practices: Use of web application firewalls. The Open Web Security Application Project, OWASP Papers Program.