# **Introduction**

As healthcare customers of today seek more flexibility, brand awareness is declining. This implies that patients who were formerly loyal to a particular healthcare provider or enterprise will transfer physicians in order to receive the service they want, and several have done so. In actuality, more than 33% of patients have switched healthcare providers in the preceding two years, citing a lack of accessibility as the primary reason for the change.

## Key Statistics for ASMIS in Healthcare

As a result of using an Appointment and Scheduling Management Information System or ASMIS, the following statistics were compiled:

* 40% of patients now consider virtual care access to be a very significant feature when choosing a provider. (Kyruus, 2020).
* 43% of patients tend to favor to arrange appointments online, a trend that continues to grow each year. (Kyruus, 2020).
* 26% of online appointments are for same-day or next-day appointments. (Mazur, 2022).
* 34% of online-scheduled appointments are made after hours. (Mazur, 2022).
* According to research, 59% of patients are irritated by waiting in queue and the awkward office hours associated with telephone appointment booking. (Hedges, 2021).

## Benefits of Adopting an ASMIS Solution

Appointment and Scheduling Management Information System will benefit the operations of a firm. In this instance, the primary advantages of using an ASMIS are:

* **Reduced Attrition:** Since scheduling is often a patient's first engagement with a healthcare office, it is essential to provide a streamlined, efficient experience that leaves a positive impression.
* **24/7 Availability:** When your office is closed and your phone lines are occupied, online scheduling is a logistical lifesaver. However, it is also convenient for patients who want the flexibility and simplicity of online appointment, regardless of the time of day.
* **Maximizes Efficiency:** Patients seeking a timely appointment may check a medical centre’s up-to-date availability of physicians without delay, often selecting those appointment spots that may go unfilled or be lost to no-shows.
* **Reduced Administrative Costs:** Online scheduling enables practise personnel to concentrate on other practice-related tasks, allowing them to achieve more throughout the workday without resorting to overtime, another factor to stress.
* **Better Patient Experience:** Employees that are less stressed then tend to concentrate on enhancing the in-office experience for patients. They have the ability to deliver a warm welcome, respond to inquiries and other in-office responsibilities.

## Potential Cyber Threats against ASMIS.

ASMIS is also susceptible to cyber-attacks and internet-based threats, including the following:

* **Injection –** An injection-vulnerable web application receives untrusted data from an input field without sufficient sanitizing. SQL injections, Email Header Injection, and other similar exploits are examples of frequent injection attacks. These attacks might result in illegal database access and the abuse of administrative rights.
* **Broken Authentication –** Broken authentication is an umbrella phrase for vulnerabilities involving improperly implemented authentication and session management mechanisms. This flawed implementation enables hackers to assume the identity of a genuine user, get access to their sensitive information, and possibly abuse the assigned ID rights.
* **Cross Site Scripting (XSS)** **–** This attack includes introducing malicious code into a web app so that it may be executed in the browsers of the victims. Successful execution leads to the compromise of user session IDs, the defacement of websites, and the routing to malicious websites.
* **Insecure Direct Object References (IDOR) –** An attacker gains foothold to database entries belonging to other accounts by tampering the URL. The vulnerability emerges when anyone can modify the URL to get unauthorised access to other similarly sensitive information.

# **Threat Model Design Approach**

The design strategy included the following steps:

* **Define Objects –** The definition of objects is the foundation of every UML diagram or DFD [data flow diagram]. A variety of shapes are used to represent different objects in a diagram, such as servers, devices, single process functions, multi-process functions, data stores, etc.
* **Define the Flow –** Once the objects have been placed in the environment, it is essential to specify their interaction flow. This flow will decide whether data will flow unidirectionally or bidirectionally between objects.
* **Define the Trust Boundaries –** Once the data flow and object interactions have been established, it is crucial to establish trust boundaries. Trust boundaries will seek to partition data flow from a single network to an interconnection of networks, where objects of varying roles and sensitivity will be separated by secure communications and controls to prevent direct interaction by unauthorised or malevolent actors.
* **Define Threat Actors –** Based on the configuration described above, threat actors may be further characterised based on an advanced persistent threat (APT) group or by location and privileges.
* **Define Criticality of Objects –** Since the whole activity is predicated on constructing a threat model, it is essential to define the criticality of diagram objects. These will offer a more accurate depiction of what is being safeguarded or what must be protected from threat actors.
* **Define Controls –** Existing controls over objects are enumerated to clarify what is being secured, if it is necessary to be secured, whether it was neglected from prior threat models, and whether the object is being protected with appropriate and efficient controls.

Organizationally, this operation is repeated multiple times for various IT infrastructure designs until an acceptable risk threshold is attained for all critical objects in consideration. This ongoing activity is also referred to as threat modelling.

# **STRIDE based Threat Modelling Approach**

A threat modelling method, such as **STRIDE**, is used to identify threats by categorising attacker objectives as shown in the table below. [Table 1]

|  |  |  |  |
| --- | --- | --- | --- |
| Property | Threat | Definition | Example |
| Authentication | **S**poofing | Impersonating an object or a person. | Impersonating to be another user, example.com or a system file and process. |
| Integrity | **T**ampering | Altering data or code | Modifying a process on disk, or a frame of packets as it traverses the LAN. |
| Non-repudiation | **R**epudiation | Denying having executed a certain activity. | “I didn’t send that email,” “I didn’t modify that file,” “I didn’t visit that web site!” |
| Confidentiality | **I**nformation Disclosure | Disclosure of confidential information to unauthorized individuals | Allowing a user to read the proprietary source code; publishing a list of confidential data to a web site. |
| Availability | **D**enial of Service | Deny or degrade service to users | Crashing a system or a web site, sending a packet and absorbing excessive CPU resources. |
| Authorization | **E**levation of Privilege | Gain capabilities without proper authorization | Allowing a remote user to execute instructions is a famous illustration. Escalating from restricted user to administrator. |

Table 1: STRIDE Threat Model with Examples.

# **UML – Threat Modelling External Threat Actors**

To illustrate external threat actors, Figure 1 will threat model the external web-application server which is used to interact with the ASMIS system, and table 2.1 the STRIDE threat modelling approach.

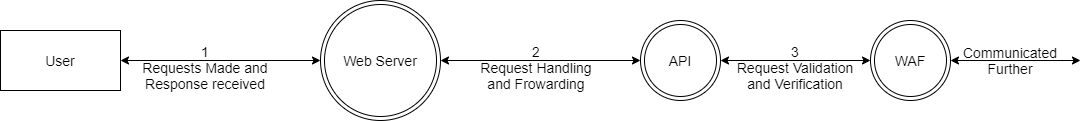


Figure 1: UML Diagram for Data Flow between user and webserver

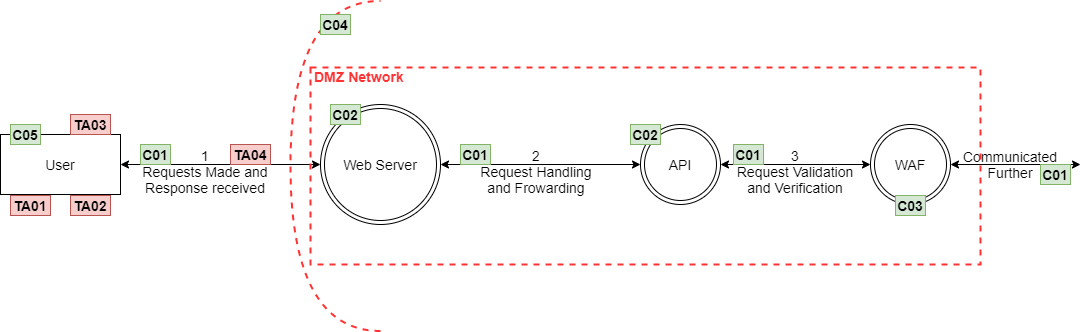
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Object** | **S** | **T** | **R** | **I** | **D** | **E** |
| Web Server | ✓ | ✓ | 🗶 | ✓ | ✓ | ✓ |
| Data Flow | ✓ | ✓ | 🗶 | ✓ | ✓ | 🗶 |

*Table 2.1: STRIDE Threat Model*

Table 2.2 as below highlights information details of the threat actors and security controls put into or planned for in place after threat modelling is completed which will enhance the overall security of the external facing device from a variety of threat actors, the controls incorporated diagram is depicted in Figure 2 on the next page.

|  |  |
| --- | --- |
| **Threat Actors (TA)** | **Security Controls (C)** |
| TA01 – External Unauthenticated User | C01 – Encryption |
| TA02 – External Authenticated User | C02 – Error Handling and Secure Configuration |
| TA03 – External Privileged User | C03 – Scanning and Validating Inputs |
| TA04 – Man-In-The-Middle | C04 – Firewall |
|  | C05 – Password-less Authentication |

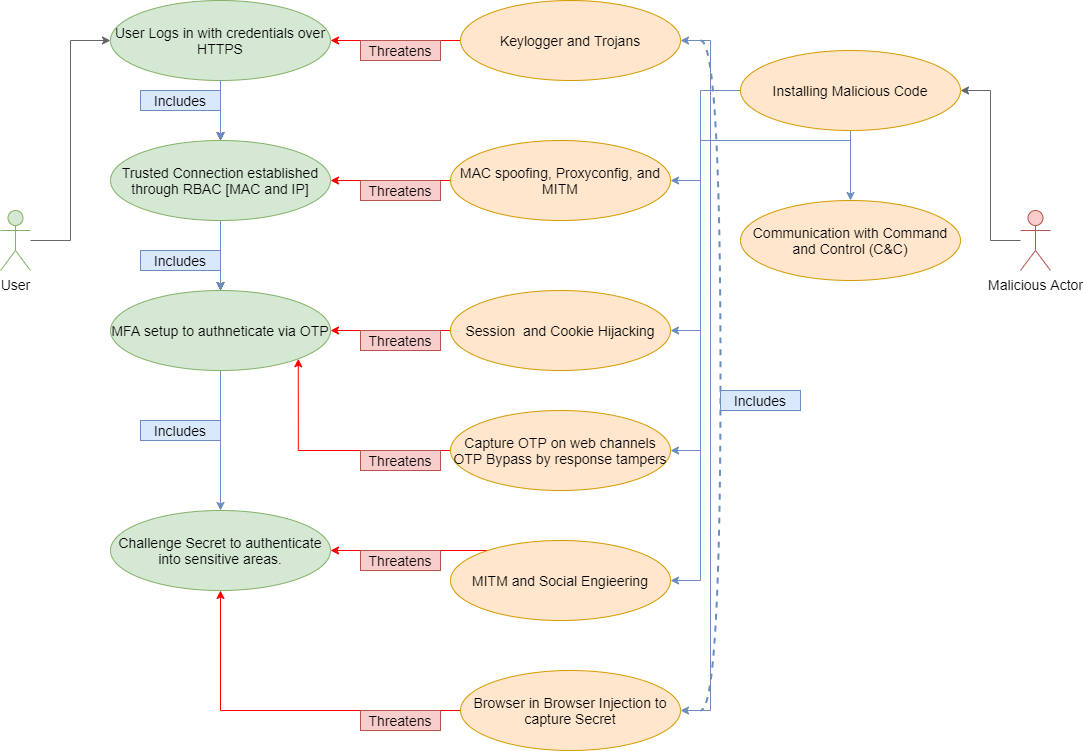
*Table 2.2: Label Information*



*Figure 2: Threat Model UML after Incorporation of Controls*

# **UML – Use/Misuse cases for Authentication**

To further illustrate the potential attacks that could be performed by an external unauthenticated threat actor [TA01] Figure 3 depicts some use cases and their misuse in relation to authentication mechanism and protections.



*Figure 3: Use/Misuse Cases for Authentication*

# **Potential Solutions**

## Next-Gen Firewall (NGFW)

A next-generation firewall (NGFW) is a security device that analyses network traffic and blocks potentially harmful traffic based on predefined rules. The capabilities of NGFWs grow and extend beyond those of conventional firewalls.

In addition to packet filtering, NGFWs utilise deep packet inspection (DPI) to protect against the following threats:

* Application awareness allows administrators to prohibit potentially dangerous apps.
* Intrusion prevention examines incoming traffic, detects known and possible dangers, and prevents them.
* Intelligence about threats is knowledge about prospective assaults. Due to the constant evolution of attack strategies and malware strains, current threat information is essential for thwarting these attempts. NGFWs are able to collect threat intelligence feeds from external sources and act on them.

Some benefits of deploying a NGFW are:

* Increased Security Standards.
* Detailed Logging.
* User Authentication and Authorization.
* Supports high level application inspection.

Some limitations of NGFW are:

* Overall high system utilization and consumption.
* Higher costs of deployment.
* Requires increased customization and fine tuning.

## Extended Detection and Response (XDR)

XDR captures and correlates data across electronic mails, desktops and systems, cloud & microservice infrastructure, and networks, providing actionable intel and insight into advanced threats. Then, threats may be evaluated, ranked, hunted, and remedied to avoid potential data loss and prevents security breaches.

Some benefits to an XDR solution are:

* Increased ability to detect stealthy attacks.
* Reduced dwell time.
* Increased speed of mitigation.

Some limitations of an XDR are:

* High overall costs.
* Unless analyzed and fine-tuned, possibilities of false positives.

## Password-less Authentication

Authentication without a password includes confirming a user's identity using anything other than a password. This might be a push notice delivered to a secondary device or a biometric identifier such as the user's face or fingerprint.

Password-less authentication removes the uncertainty from safe, frictionless authentication – a need that is growing in importance due to the increased activity of going “online”. Seamless authentication fosters confidence and may increase conversion rates. Eliminating passwords also increases data security by thwarting hostile login attacks.

Some benefits to a password-less authentication mechanism are:

* Improved user experience.
* Increased security.
* Reduced administration overheads.

Some limitations of password-less authentication mechanism are:

* Potentially increased costs.
* Harder to troubleshoot.

## Hashing and Encryption

The operation of hashing converts a given key to another value. The new value is generated using a hash function in accordance with a mathematical method. The outcome of a hash function is referred to as a hash value or hash for short.

Encryption is a technique for encrypting data so that only authorised parties may decipher it. In technical terms, it is the process of transforming plaintext into unintelligible text, also known as ciphertext. Encryption, in plain words, restructures readable data so that it projects to be random. Encryption necessitates the employment of a cryptographic key: a set of mathematical values that both the sender and the receiver of an encrypted communication agree on.

Some benefits of data encryption and hashing are:

* Encryption guarantees that no one other than the intended receiver or owner of the data may read conversations or data at rest.
* Encryption prevents data breaches regardless of whether the data is in transit or at rest. If a business device's hard disc is correctly encrypted and it is lost or stolen, the data on that device will remain safe.
* Encryption also prevents hostile behaviour such as on-path assaults, which may compromise data integrity.

Some limitations:

* Unquestionably, data encryption is a massive undertaking for an IT professional. The greater the number of data encryption keys, the more challenging it may be for IT administrators to keep all of the keys. If the encryption key is lost, the data connected with it is also gone.
* Data encryption may be fairly expensive due to the need for capacity and modifications on the part of the systems that maintain the encryption. Without suitable systems, the efficiency of system operations may be degraded greatly.
* Unrealistic Standards and Requirements: If an organisation does not comprehend some of the limitations imposed by data encryption technology, it is simple for it to establish unrealistic standards and requirements that might compromise the security of data encryption.
* Integrating data encryption technologies with current programmes and applications may be challenging. This may adversely impair the system's everyday functions.

**References**

* A BETTER MATCH\_ MEANS BETTER CARE® Insights from Kyruus’ Annual Survey of 1,000 Healthcare Consumers INTRODUCTION: RE-IMAGINING THE PATIENT JOURNEY TO ACCESSING CARE. (2020). Available from: https://www.kyruus.com/hubfs/Kyruus%20Patient%20Access%20Journey%20Report%202020.pdf?hsLang=en [Accessed 8 May 2022].
* Auth0. (n.d.). Auth0 | 7 Things You Need to Know About Passwordless Authentication. Available from: https://auth0.com/resources/whitepapers/passwordless-authentication [Accessed 8 May 2022].
* cheatsheetseries.owasp.org. (n.d.). Threat Modeling. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Threat\_Modeling\_Cheat\_Sheet.html [Accessed 9 May 2022].
* Cloudflare. (n.d.). What is a next-generation firewall (NGFW)? Available from: https://www.cloudflare.com/en-in/learning/security/what-is-next-generation-firewall-ngfw/ [Accessed 9 May 2022].
* Cloudflare. (n.d.). What is Encryption? Available from: https://www.cloudflare.com/en-in/learning/ssl/what-is-encryption/ [Accessed 9 May 2022].
* Conklin, L. and Drake, V. (2021). Threat Modeling Process | OWASP. owasp.org. Available from: https://owasp.org/www-community/Threat\_Modeling\_Process [Accessed 9 May 2022].
* criticalmedia.co.uk, C.M. - (2020). Passwordless authentication: pros and cons. Condatis. Available from: https://condatis.com/news/blog/passwordless-authentication-pros-and-cons/.
* Educative: Interactive Courses for Software Developers. (n.d.). What is hashing? Available from: https://www.educative.io/edpresso/what-is-hashing [Accessed 9 May 2022].
* Eira, A. (2019). 74 Basic Appointment Scheduling Statistics: 2020/2021 Data Analysis & Market Share. Financesonline.com. Available from: https://financesonline.com/appointment-scheduling-statistics/ [Accessed 9 May 2022].
* Hedges, L. (2021). [Research] Online booking options can get you more clients. GetApp. Available from: https://www.getapp.com/resources/research-online-booking-importance-of-appointment-scheduling/ [Accessed 9 May 2022].
* Knight, A. (2018). Threat Modeling of Connected Cars using STRIDE. Medium. Available from: https://alissaknight.medium.com/threat-modeling-of-connected-cars-using-stride-e8184764eb0a [Accessed 8 May 2022].
* Kyruus (2020). 2020 Patient Access Journey Report | Kyruus. www.kyruus.com. Available from: https://www.kyruus.com/2020-patient-access-journey-report-lp [Accessed 7 May 2022].
* Mazur, C. (2022). 21 Appointment Scheduling Statistics [2022]: Online Booking Trends – Zippia. Zippia. Available from: https://www.zippia.com/advice/appointment-scheduling-statistics/ [Accessed 9 May 2022].
* PatientPop. (n.d.). 5 benefits of online scheduling for healthcare practices. Available from: https://www.patientpop.com/whitepapers/3-benefits-of-online-scheduling/ [Accessed 9 May 2022].
* SentinelOne. (n.d.). What is XDR? Available from: https://www.sentinelone.com/cybersecurity-101/extended-detection-response-xdr/ [Accessed 8 May 2022].
* Shostack, A. (2007). STRIDE chart - Microsoft Security. Microsoft Security. Available from: https://www.microsoft.com/security/blog/2007/09/11/stride-chart/ [Accessed 9 May 2022].
* Spamlaws.com. (2019). The Pros and Cons of Data Encryption. Available from: https://www.spamlaws.com/pros\_cons\_data\_encryption.html [Accessed 9 May 2022].
* The Windows Club. (2022). Different types of Firewalls: Their advantages and disadvantages. Available from: https://www.thewindowsclub.com/different-types-of-firewalls [Accessed 8 May 2022].