X Embassy Threat Model

Owner: Hadeer Amr 22010450
Reviewer: Akmal Ibrahim
Contributors: Rewan Salah 20221447143, Marwan Ashraf 20221311732, Aya Mohamed 20221380245, Abdelraman Raslan 20221460102
Date Generated: Sat May 10 2025

Executive Summary

High level system description

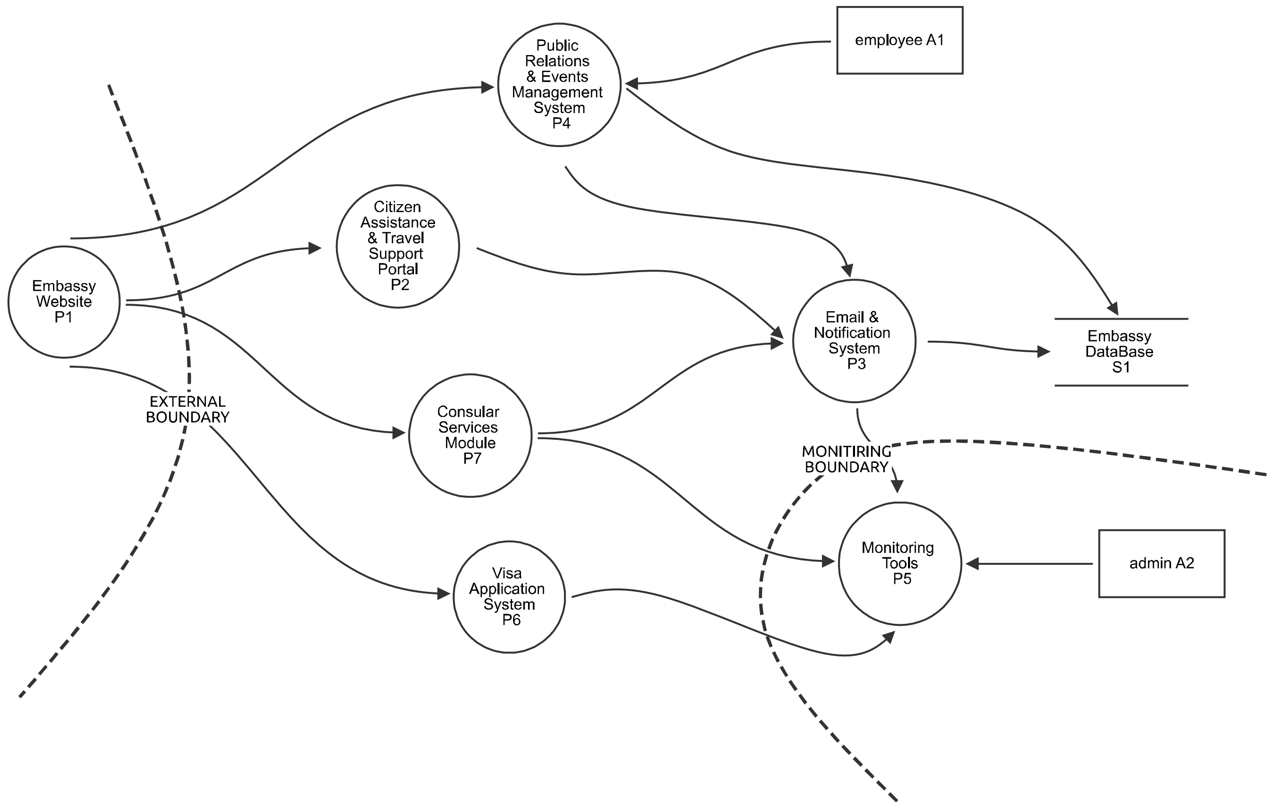
The Embassy of X in YY is the official diplomatic mission representing X’s government and citizens in YY. Located in YY, the embassy provides a wide range of consular services including visa issuance, passport renewal, and assistance to X nationals residing or traveling in YY. It also works to strengthen political, economic, cultural, and educational ties between the two countries.

The embassy serves as a vital bridge for bilateral cooperation, supporting trade partnerships, hosting cultural events, and facilitating dialogue on shared interests. With a team of trained diplomats and support staff, the Embassy of X is committed to promoting mutual understanding and protecting the rights and interests of X citizens abroad.

Summary

Total Threats	22
Total Mitigated	22
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram


Public Relations & Events Management System P4
employee A1
Citizen Assistance & Travel Support Portal P2
Embassy Website P1
Email & Notification System P3
Embassy DataBase S1
EXTERNAL BOUNDARY
Consular Services Module P7
MONITIRING BOUNDARY
Monitoring Tools P5
admin A2
Visa Application System P6

New STRIDE diagram

employee A1 (Actor)

Description: embassy staff member

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	Cracked Software Vulnerability	Spoofing	High	Mitigated		An embassy staff member installs unauthorized cracked software on an internal workstation. The software contains a backdoor that allows an attacker to infiltrate the internal network. Once inside, the attacker moves laterally across systems, escalates privileges	Enforce strict software policies as blocklisting ensure monitoring and detecting unauthorized software installations make sure of regularly patch and update systems you can isolate sensitive networks and use endpoint detection & response (EDR) and conduct awareness training for employees on the risks of pirated software
19	Insider Threat by Malicious Employee	Repudiation	High	Mitigated		Employee misuses authorized access to extract sensitive citizen data such as passport numbers, visa records, or diplomatic communication. They may leak the data intentionally or sell it to third parties. Since this is a legitimate user, their actions may go unnoticed or be hard to trace	Apply least privilege access control and enable user behavior analytics (UBA) and anomaly detection and log and monitor all user activity.

Embassy DataBase S1 (Store)

Description: to store information like visa applications, citizen data, appointments

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Unencrypted Data at Rest	Information disclosure	Critical	Mitigated		Sensitive data like visa records, birth certificates, and personal IDs are stored unencrypted in the database or local files	Enable full-disk encryption or row-level database encryption using strong algorithms as AES-256
29	Privilege Misuse	Tampering	Critical	Mitigated		An insider with legitimate access may intentionally or accidentally alter or delete critical records leading to loss of integrity and service disruption. This could go undetected without proper logging and auditing.	Implement robust logging and audit trails for all database operations and enforce Role-Based Access Control (RBAC) and least privilege
30	ransoware attack	Denial of service	Critical	Mitigated		attacker inside network deploy ransomware	keeping regular backup on another place perfered more than 1 backup hardcopy and softcopy ensure monitoring and logging

Embassy Website P1 (Process)

Description: Website used by citizens and travelers to access embassy services online

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	SQL Injection in Web Portal	Tampering	Critical	Mitigated		Malicious SQL code is injected through user inputs	Use parameterized queries and ensuring input validation and sanitization
10	Brute Force attack	Spoofing	High	Mitigated		Repeated login attempts using automated guessing	Implement account lockouts, 2FA, and IP blacklisting

Number	Title	Type	Priority	Status	Score	Description	Mitigations
27	Cross-Site Scripting XSS	Tampering	High	Mitigated		The website allows unvalidated input in fields as forms and search enabling attackers to inject malicious scripts. This can lead to session hijacking, defacement, or data theft	Implement input validation and output encoding and apply Content Security Policy (CSP) headers

admin A2 (Actor)

Description: embassy staff 2

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Spear Phishing	Spoofing	High	Mitigated		An attacker targets a system administrator with a phishing email that imitates an internal embassy IT notice. The admin unknowingly enters their credentials on a fake login page. The attacker then uses these credentials to gain administrative access to embassy systems, modify permissions, disable logging, or deploy malware.	Enforce Multi-Factor Authentication (MFA) for admin accounts and provide phishing awareness training and use privileged access management (PAM) systems.
21	Voice Impersonation via Deepfake	Repudiation	Low	Mitigated		A voice deepfake of an admin is used over phone/email to request unauthorized changes to records.	enforce policy restrict sensitive actions to be performed only through authenticated admin portals never based on audio/email requests alone and train all staff and require all sensitive requests to be verified through a secure multi-step process

Monitoring Tools P5 (Process)

Description: to check system performance and detect any problems

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Log Forgery Attack	Tampering	High	Mitigated		Attack alters system logs to hide traces of intrusion	using PAM to monitor Privileged accounts in the system also make sure of implementing MFA restrict access to log files and implement centralized logging
22	Log Flooding Attack	Denial of service	Critical	Mitigated		An attacker floods the embassy's monitoring tools with excessive fake logs, error messages, or alerts. This overwhelms the system, consumes storage and CPU, and hides real malicious activities under the noise.	Implement log ingestion rate limits per source to prevent abuse and sanitize and normalize log input to avoid fake or malformed entries

Email & Notification System P3 (Process)

Description: ends updates to users (like appointment confirmation or document requests)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Notification Spam Attack	Denial of service	Critical	Mitigated		Email system overwhelmed by fake alerts, delaying real notifications	using backup server and implement rate limiting IPS can be used to stop and detect malicious upnormal activities also implementing firewall and strict rules
9	Email Spoofing Attack	Spoofing	High	Mitigated		Attackers send phishing emails impersonating the embassy	Educate users and give them good training monitor for impersonation

Visa Application System P6 (Process)

Description: Visa Application System. This system is responsible for receiving and processing visa applications submitted from the embassy's website (P1).

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Authentication Bypass	Repudiation	High	Mitigated		Authentication bypass occurs when an attacker is able to access a system or service without proper login credentials. This may be due to insecure session management, logic flaws in authentication routines, poorly protected admin endpoints, or disabled checks in development environments.	Use secure session management Conduct regular security testing Implement MFA for both users and admins
13	Error Handling Vulnerability	Information disclosure	Critical	Mitigated		System exposes overly detailed error messages to the end user, it unintentionally reveals internal workings of the system. This help an attacker understand the system architecture, discover technology stacks , identify potential injection points and find admin paths and database names.	Show generic error messages to end users and set proper error reporting levels in server configuration and sanitize inputs and filter outputs to prevent sensitive data from leaking via APIs or UI.

Public Relations & Events Management System P4 (Process)

Description: Public Relations and Events Management. Responsible for managing public activities, parties, conferences, or any event organized by the embassy. A1 staff member directly interacts with the office.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	DNS Spoofing	Tampering	Critical	Mitigated		DNS spoofing (also known as DNS cache poisoning) is an attack where an attacker redirects legitimate user traffic to a fake website by manipulating DNS records. For example, a user trying to access visa.embassy.gov may unknowingly be sent to a malicious clone site controlled by an attacker. This is commonly used to harvest credentials or spread malware.	Use DNSSEC to secure DNS queries and prevent tampering Monitor DNS records for any unauthorized changes or suspicious activities. Regularly update DNS server software and configurations to minimize vulnerabilities
24	Unintentional Information Exposure via Public Communications	Information disclosure	Low	Mitigated		During public communications such as press releases, social media announcements, or stakeholder briefings, sensitive technical or procedural information may be unintentionally revealed this is a real-world threat that attackers can exploit during the reconnaissance phase to craft more tailored attacks and exploit known infrastructure components.	Establish and enforce a Communications and Social Media Policy for all staff and implement an approval workflow for all public communications

Citizen Assistance & Travel Support Portal P2 (Process)

Description: This module focuses on providing emergency support and assistance for citizens abroad. It manages requests for help, travel-related queries, and emergency contact procedures. It communicates with the Email & Notification System to send alerts or assistance confirmations to both citizens and internal staff. It can also retrieve or update case-related information stored in the central database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Abusing Misconfigured Permissions	Tampering	High	Mitigated		An employee accesses and leaks personal user data	Automate Misconfiguration Detection Enforce Periodic Access Reviews Apply the Principle of Least Privilege (PoLP) Implement Role-Based Access Control (RBAC)
26	Man-in-the-Middle Attack	Tampering	High	Mitigated		An attacker intercepts and possibly modifies data in transit between external users and embassy systems.	Enforce strong TLS/SSL encryption and ensure secure authentication as OAuth2

Consular Services Module P7 (Process)

Description: The Consular Services Unit provides services such as issuing official documents, birth or death certificates, notarizations, etc. It also operates in parallel with other systems.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	Unpatched System	Elevation of privilege	High	Mitigated		The Consular Services module is running outdated software that contains known vulnerabilities. Attackers may exploit these to gain unauthorized access, modify records and escalate privileges within the system.	Regularly apply security patches and updates automatic update alerts and centralized patch management Conduct periodic vulnerability assessments
28	Broken Access Control	Tampering	High	Mitigated		A compromised user account or misconfigured access may allow unauthorized changes to consular documents or services, such as forged travel documents or appointment manipulation.	Implement RBAC enforce separation of duties enable multi-factor authentication for sensitive operations