SAPI-G
Secure API Gateway with AI Threat Detection

Phase 2: Threat Modeling & Risk Assessment

Secure Software Development
CY-321

Project Team:
Umar Tariq (2022604)
M Zeeshan (2022644)
Ayela Israr (2022130)
Ahmad Amjad (2022063)

Threat Modeling & Risk Assessment

---

1. Attack Vectors

Below are potential attack vectors that could target the Secure API Gateway:

1.1. Injection Attacks

- **Description: Attackers may exploit SQL, NoSQL, or Command Injection vulnerabilities.**
- **Impact: Unauthorized data access, data manipulation, or database compromise.**
- **Example: Malicious input altering an SQL query to dump sensitive data.**

1.2. API Abuse & Rate-Limiting Bypass

- **Description: Attackers may exploit unrestricted API access to overload the system.**
- **Impact: Denial of service, resource exhaustion, and performance degradation.**
- **Example: A bot repeatedly making API calls to consume all available bandwidth.**

1.3. Authentication & Session Hijacking

- **Description: Attackers might steal session tokens or exploit weak authentication mechanisms.**
- **Impact: Unauthorized access to sensitive resources.**
- **Example: Session replay attacks using stolen JWT tokens.**

1.4. Man-in-the-Middle (MitM) Attacks

- **Description: Intercepting API communication to alter or steal data.**
- **Impact: Data breaches and integrity compromise.**
- **Example: Eavesdropping on unencrypted API traffic.**

1.5. Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF)

- **Description: Injecting malicious scripts into API responses or forcing users to execute unintended actions.**
- **Impact: Account takeover and data exfiltration.**
- **Example: A malicious script capturing API tokens from a user session.**

1.6. Insider Threats

- **Description: Malicious insiders exploiting privileges to access sensitive data.**

- **Impact: Unauthorized data exposure and system compromise.**
- **Example: A disgruntled employee leaking API keys.**

---

2. Risk Levels & Mitigation Strategies

The following table categorizes each attack vector by risk level and the corresponding mitigation strategies:

Attack Vector	Risk Level	Mitigation Strategies
Injection Attacks	**High**	**Input validation, parameterized queries, WAF rules**
API Abuse & Rate-Limiting Bypass	**High**	**API rate limiting, IP blacklisting, anomaly detection**
Authentication & Session Hijacking	**High**	**Multi-factor authentication (MFA), token expiration**
Man-in-the-Middle (MitM) Attacks	**High**	**HTTPS/TLS enforcement, mutual TLS authentication**
Cross-Site Scripting (XSS)	**Medium**	**Input sanitization, Content Security Policy (CSP)**
Cross-Site Request Forgery (CSRF)	**Medium**	**CSRF tokens, SameSite cookie enforcement**
Insider Threats	**Medium**	**Least privilege access control, audit logs**

3. Security Mitigation Strategies

3.1. Secure Authentication & Authorization

- **Implement OAuth 2.0 and JWT for secure authentication.**
- **Enforce MFA for privileged API access.**

- **Implement Role-Based Access Control (RBAC).**
- **Use short-lived JWTs with automatic token refresh mechanisms.**

3.2. API Security Controls

- **Enforce rate limiting using API Gateway policies.**
- **Block requests from malicious IPs via IP blacklisting.**
- **Implement request/response validation mechanisms.**
- **Deploy API anomaly detection using AI-based monitoring.**
- **Implement API key rotation and automated revocation policies.**

3.3. Network & Communication Security

- **Enforce HTTPS for secure data transmission.**
- **Implement TLS mutual authentication for trusted communication.**
- **Monitor network traffic for anomalies using AI-powered threat detection.**
- **Use a Web Application Firewall (WAF) to block suspicious requests.**

3.4. Data Protection & Logging

- **Encrypt sensitive data at rest and in transit.**
- **Implement real-time logging and alerting for security incidents.**
- **Store logs securely and analyze them for potential breaches.**
- **Use tamper-proof logging mechanisms for forensic investigations.**

3.5. Continuous Monitoring & Threat Intelligence

- **Deploy intrusion detection and prevention systems (IDS/IPS).**
- **Use AI-powered anomaly detection to identify potential threats.**
- **Regularly update API security policies based on new threat intelligence.**
- **Conduct regular security audits and penetration testing.**
- **Automate security patching and updates.**