

CASE STUDY



macro global[®]
creating value through innovation



Protecting APIs Against Security Threats

API

Application
Programming
Interface

Synopsis

Open Banking offers financial institutions an opportunity to gain a competitive edge by providing customer-focused financial services with enhanced user experience. The potential impact on the market landscape and the size of opportunity empowers the financial institutions to consider the strategic directive, Open Banking. On the other hand, compliance with Open Banking introduces technical challenges and mandates enhanced security controls to ensure sensitive data is not misused or not shared legally. Open Banking brings in potential threats, such as security risks in exchanging data between third-party providers (TPPs) and banks (ASPSP) or hacked requests made via TPPs that may be vulnerable to third party fraud driven by malware.

This case study enables the readers to think through the potential security challenges faced by the banks in API management and how Macro Global's Tavas – Open Banking Product Suite and solution benefitted our clients with comprehensive governance framework and control measures to mitigate risk.

Background

The market changes create new risks of fraudulent activities since banks are mandated to allow regulated third-party providers to access customer financial information as mandated by the Open Banking Regulations. The rules of the security game are changing profoundly, and banks are engaged in a race to remain ahead of more sophisticated cyber-criminals and attacks.

A whole host of opportunities are created for fraudsters as banks implement API and open their infrastructure to TPPs which impacts the visibility when it comes to end-to-end transaction monitoring and inevitably affects their ability to prevent and detect fraudulent transactions. Payment service users (PSU) may no longer need to log on to their digital banking thereby reducing the amount of relevant data required for banks. Against the subjected background, providing a secure infrastructure to TPPs is a major challenge for banks and failing to implement an architecture that mitigates threats could result in significant financial and reputational loss. To get rid of malicious denial-of-service attacks, the banks are expected to have a rate-limiting mechanism to set the threshold on the maximum number of requests made per day and appropriate encryption techniques to prevent the banks from the man-in-the-middle attacks. Hence, payment service providers and banks have realised that current industry standards for network security and secure transmission are not sufficient and require 'future-proof' security that allows banks and TPP to harden the existing services to withstand today's dynamic threats.

Three security challenges that banks need to consider:



Security Challenges

The architecture and design of APIs are generally employed as HTTP protocol and banking applications are increasingly composed of rich mechanisms that connect to back-end RESTful APIs (e.g., micro-services, web services) over HTTP using JSON to exchange/transfer data. APIs are vulnerable to many security threats which might result in corruption or destruction of sensitive user data, leakage of sensitive data, or unauthorised financial transactions.

Attacks are typically carried out on websites and web applications with APIs implicitly inclined to most common web-related threats such as injection attacks leading to the loss of personal information, man-in-the-middle attacks resulting in interception of transaction data and Denial-of-Service attacks compromise the quality availability of service for users. The subjected attacks are especially pertinent where existing services have been turned outwards to face the Internet with an API, as there is the potential for existing security weaknesses.

Injection Attack

Injection vulnerabilities give a pathway to attackers to bypass the authorisation and authentication stages of web pages and security checkpoints. Injection attacks occur when data is shared between the bank and third-party provider (ASPSP) as part of an API function call. The attacker's malicious data can trick the exponent by executing unintended commands or accessing the data without proper consent. An example of such an attack is SQL injection, whereby malicious SQL statements gaining access to sensitive financial or personal data stored on the SQL databases results in an adversary effect by modifying or deleting the information stored on the target database servers.



HTTP Parameter Pollution (HPP) Attack

HTTP Parameter Pollution (web attack evasion technique) is performed by polluting HTTP GET/POST requests by injecting multiple parameters with the same name holding different values. The attacker creates an HTTP request to manipulate or retrieve hidden information upon receipt of the API function call resulting in fraudulent action. HPP attack is exploited by the attacker or hacker in order to bypass pattern-based security mechanisms by initiating a fraudulent transaction whereby money is deducted from the bank account without customer authorisation/knowledge.



Denial-of-Service (DoS) Attack

A Denial-of-Service attack (cyber-attack) affects the availability of API and aims to disrupt the service by interrupting normal functioning. APIs are potentially open to flooding and types of DoS attacks halt the back-end systems or services resulting in downtime for banking operations and transactions. The malicious attempt disrupts the normal traffic of a targeted server, service, or network by overwhelming the target or infrastructure with a flood of Internet traffic and DoS attack the API by overwhelming the request if an API has no limitations on the number of resources.



Authentication and Session Attack

Another common API vulnerability is the use of illegitimate tokens to gain access to service endpoints. Broken Authentication is the vulnerability or weakness inherited in the online platform or application permitting attackers to bypass the login security and the attacker could hijack the user session if the session token is exposed in the URL and the attacker obtains the hyperlink with excessive privileges. Application functions related to authentication and session management are rarely implemented erroneously enabling hackers to compromise login credentials/passwords which leads to hijacking the details and access/modify the information for which the hacker has no permission. For instance, if the bank hasn't validated the certificate of TPP using its API, TPP could obtain financial information about customers of the bank or even initiate fraudulent transactions.



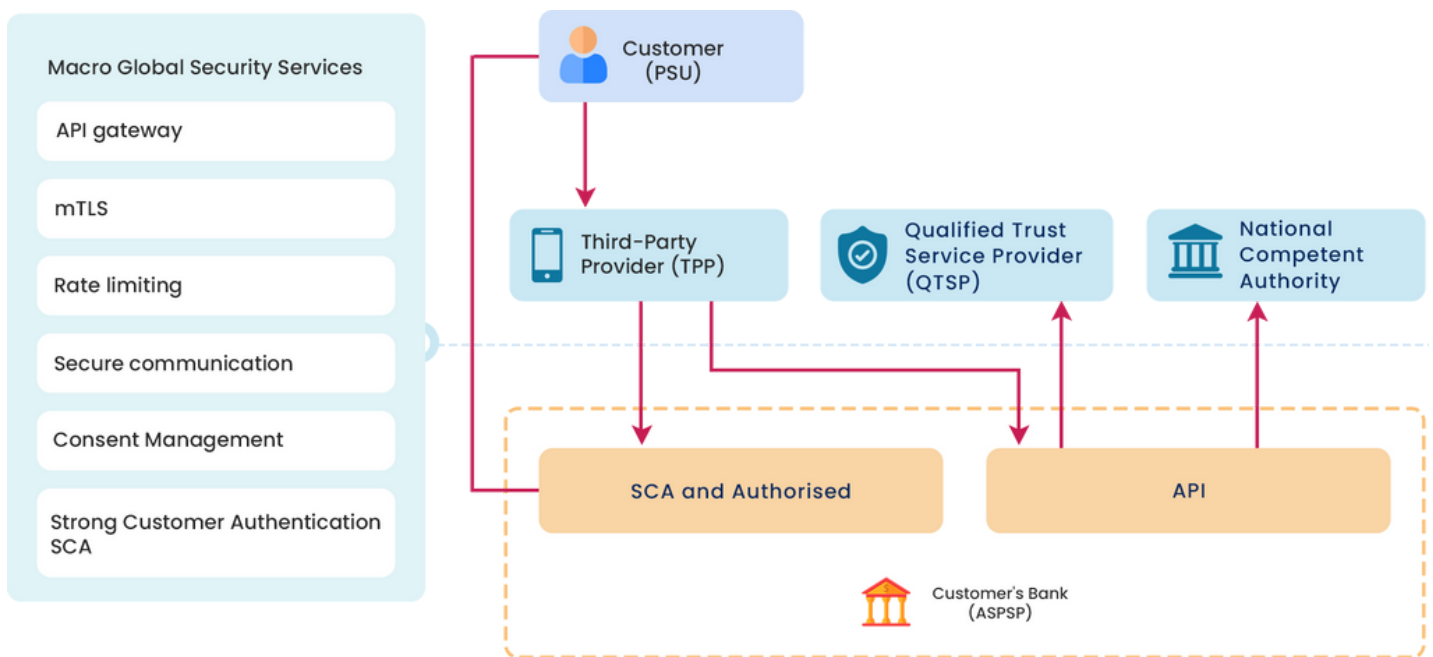
Man-in-the-middle Attack

Man-in-the-middle attack intercepts communications between a customer's device and the banking sector and enables attackers to manipulate/interfere with legal API requests/responses. The attacks usually occur because requests and responses were not exchanged via a secure channel (e.g., SSL/TLS), or the secured channel is not authenticated. For instance, SSL/TLS might be implemented without certificates allowing the bank or TPP to be spoofed by altering the IP address and as a result, users attempting to access a URL connected to the application are redirected to the attacker's website. SSL/ TLS might also be implemented without HTTP Strict Transport Security (HSTS) allowing a redirection attack from HTTPS to plaintext HTTP.



What we did – Security Enforcement and Risk Reduction

Security is the most important factor when it comes to API management and when exposing APIs to the external world. Macro Global adopted a number of technical and organisational security measures to address security threats against their APIs. Macro Global as a Technical Service Provider (TSP) ensured the communication channel between the banks (ASPSP) APIs and the third-party providers (TPP) using secured encryption by minimising the leakage of sensitive data and unauthorised financial transaction. Macro Global's stringent data security approach across the Open Banking platform simplifies the integration and is compatible with industry practices such as Financial-grade API (FAPI) and Mutual TLS (mTLS). Mitigation measures and control mechanisms are considered in Tavas to manage security threats.



API Management

Macro Global's API Management works with Token Server to enforce the scope of authorised access by enabling data access only for an explicitly granted application and delivers protocol intervention and consumer identity. The most common security requirement is achieved via OAuth 2.0 tokens, basic authentication, and API keys. OAuth 2.0 tokens provide greater flexibility and security to manage the validity of the tokens. API Management delivers protocol mediation with metered and governed boundaries between the security gateway to limit the impact to existing services when exposing external APIs.

Rate Limiting

Rate limits on APIs using an API gateway to determine how many requests should be allowed per subscriber in order to protect the backend services from high authorised loads. Secured API access by dropping or denying specific requests by validating the headers, parameter values etc. Rate limits and quotas are applied providing end-to-end security and API policies are defined on per-endpoint basis enabling banks (ASPSP) to perform the required authentication.

OAuth 2.0 and OpenID Connect

Dedicated Identity Server supports common API security standards such as OpenID Connect (OIDC) standard protocol built on top of OAuth 2.0 used for Identity and Access Management to face off the data privacy challenge. Our API Gateway provides API management and authenticates requests using API access token instead linked with customer details to prevent unauthorised access. OAuth 2.0 Token Binding binds access token and/or authorisation code to TLS connection to thwart attackers from hacking the authorisation code.

Secure Communication

Secure Socket Layers (SSL)/ Transport Layer Security (TLS 1.2) security standards provide high-quality standards for common and secure communication as mandated by Regulatory Technical Standards (RTS). HTTPS enables authentication and encryption of transactions between the payment service user and bank (ASPSP) and vice versa by securing the connections, infrastructure, and private keys. The Content-Security-Policy and X-XSS protect API communications from SQL Injection and Cross-Site scripting.

FAPI Compliance

Macro Global's Tavas – Open Banking Product Suite and Solution is fully Financial-grade API compliant with an advanced approach which enables secure exchange of customer financial information amid stronger security, openness, and flexibility. For a security and audit perspective, additional headers are defined to provide a consistent identifier across the communication.




JWT (JSON Web Tokens) & Proof Key for Code Exchange

Macro Global's Open Banking payment workflow is secured with a signed JSON Web Tokens (JWT) an open standard (PS256) and digitally signed using a secret key pair for secure transmission and communication between the third-party providers (TPP) and the bank (ASPSP) as a JSON object. The proof key for Code Exchange prevents the attacker from using the access token shared to the payment service user on a mobile device since the key becomes invalid after a particular period of time.

Security Governance Framework

Macro Global's API Gateway ensure the availability of the financial institution's API and maximises the scalability and reliability of the underlying authentication, authorisation and control of requests. In order to protect against security threats, the API software component parsing that data structures are hardened against attack and also protect input refinement to prevent injection in all forms. Our solution is enriched by optimising governance, risk management, and cybersecurity with advanced analytics.

Business Continuity

-  Business Continuity Management plan to avoid service losses
-  BCM/contingency plans to avoid disruption and recover from failures
-  Test BCM plans at least annually, and update based on results

Security Measures

- 💡 Operational and security risk management framework.
- 💡 Policies, procedures, and systems to identify, measure, monitor and manage risks and continuous monitoring of threats and detection.
- 💡 Investigate anomalous activities and risk assessments of functions and processes
- 💡 Preventative security measures
- 💡 Protect sensitive data in storage and transmission – confidentiality and integrity on data and systems
- 💡 Strong controls over privileged access – Strong Customer Authentication (SCA)
- 💡 Detective measure for malware, security threats public vulnerabilities/patches
- 💡 Monitoring and reporting of operational or security incidents
- 💡 Define thresholds/events/indicators for security incidents

Testing of Security Measures

- 💡 Vulnerability and Penetration Testing to check robustness and effectiveness of controls to reflect threats
- 💡 Verification of service providers, authentication devices and user code.
- 💡 Monitoring and update security based on testing outputs



Our Success Story



Enhancing the bank's overall security posture with real-time monitoring of transaction risks and support the financial institution in complying with Open Banking Regulations.



Open Banking APIs are protected through a control mechanism and the firewalls/proxy server provide broad protection against the distributed denial-of-service (DDoS) attacks.



Multi-layered controls to better respond to the security challenges and maintain the accurate level of availability and performance.



Provide secure communication interfaces and security control measures to protect the interfaces and customer financial information against threats.



Real-time analytics and reporting enable financial institutions and third-party providers to trace the events relevant to API usage.



Incident Management procedures and standards to reflect the connectivity between TPPs and financial institutions.

We are here to help you

If you want to learn more about our products or services or just have a question?

If you need advise from our expert team who understand your business better than our peers?

If you want to know how we transformed businesses using our unparalleled industry and domain expertise?

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

<https://www.macroglobal.co.uk/contact-us/>

