WHITE PAPER

GSMA Open Gateway: Cybersecurity Considerations and Solutions

Executive Summary

Mobile network operators (MNOs) have made colossal investments in 5G networks and are continuously looking for ways to monetize their 5G assets to drive return on investment (ROI) and growth. Exposing network capabilities and information has a potential high monetary value as it will drive innovation and a higher level of network customization for enterprises and application developers.

GSMA's Open Gateway initiative[1] aims to standardize network APIs that the telecom industry can offer application developers and its application ecosystem to harmonize revenue-generating interactions.

Regardless of a connected device location and to which MNO network it is connected, GSMA's Open Gateway initiative allows applications to use the same application programming interfaces (APIs) to send an SMS for two-factor authentication to know the whereabouts of an Internet-of-Things (IoT) device, to check if a subscriber has recently changed their SIM card, or to charge their mobile account for a service, and more.

While API exposure facilitates network monetization opportunities, it also enlarges the mobile network's attack surface by creating new attack vectors. Numerous examples of API-based attacks on MNOs demonstrate that exposing APIs, even to a handful of trusted partners, comes with a risk that must be mitigated via cybersecurity.

Introduction

Different MNOs would design and implement different APIs (also known as API fragmentation) for the same service, a practice that has often led to high integration costs for partners and application developers that want to build an application or service to be used worldwide. This complexity and high costs resulted in enterprises' and developers' reluctance to deliver innovation through a tighter integration and consumption of telco network capabilities, services, and information.

To try and resolve this issue, GSMA has created the Open Gateway initiative. GSMA Open Gateway is a framework of common network APIs designed to provide universal access to operator networks for developers to help developers and cloud providers enhance and deploy services more quickly across operators via single points of access to mobile networks and services. It seeks to facilitate the transformation of mobile networks into value-add and Network-as-a-Service (NaaS) platforms, making telco's capabilities available for consumption in an interoperable and programmable way.

GSMA Open Gateway API	API Functionality
SIM Swap	The API checks the last time the SIM card associated with a mobile number (MSISDN) has changed.
Quality On-Demand	The API requests a stable latency or throughput for specified application data flows.
Device Status	The API checks the connectivity status for the user equipment.
Number Verification	The API enables the seamless authentication of the mobile device by the mobile network.
Simple Edge Discovery	The API allows an application to discover the nearest edge-cloud node for it to connect to.
One-Time Password SMS	The API delivers a short-lived one-time password to a device's number via SMS to provide a proof of possession of the phone number.
Carrier Billing: Check Out	The API allows the purchase of digital goods from an online merchant and to request payment against the user's operator billing account.
Device Location	The API allows an application to check if a mobile device is near a given location.

Table 1: Summary of the APIs included in GSMA Open Gateway

Open Gateway defines a limited set of APIs for exposing network capabilities to become a universal API for all MNOs worldwide. The goal is that software developers would only need to compile their applications against a single API used by any MNO that adheres to the GSMA Open Gateway initiative. A significant and representative number of MNOs have already signed with the project, and more are expected to sign in the future, to have a level of interoperability similar to international roaming.

The GSMA Open Gateway initiative launched with several network APIs, as shown in Table 1, with plans to launch further APIs to extend NaaS capabilities, enhancing the dynamic and consumable nature of the mobile network and its capabilities.

The Dark Side of APIs

APIs provide the agility to deliver innovation, value, and growth. APIs can expose the very heart and brains of the networks and their data as to provide the agility and flexibility required to harness the mobile network's capabilities.

The same critical exposure can be intentionally or unintentionally abused. Malicious actors (hackers and nation-states) may use the APIs to exfiltrate sensitive subscriber and network data, target specific users, or commit fraud and abuse of the service.

This is not a hypothetical case, as numerous attacks have taken place using unprotected or vulnerable APIs of leading mobile operators. Some examples of these attacks have been documented by the press, resulting in significant financial and reputation losses.

Exposing APIs, including the GSMA Open Gateway APIs, without proper protection can lead to losing any advantage and monetization gained by the exposure itself. Appropriate mitigation must be put in place via the implementation of API cybersecurity.

Securing APIs

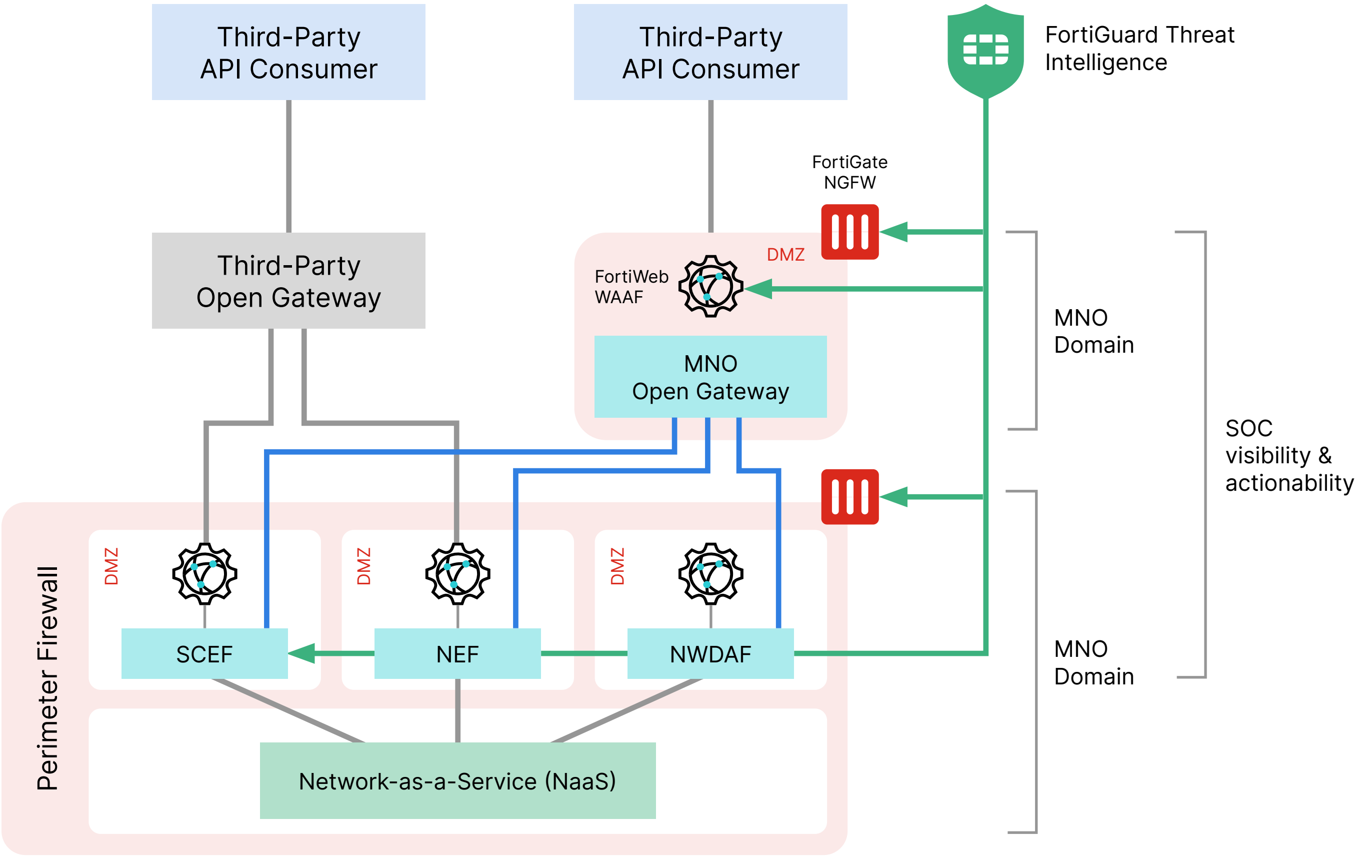
Using an API gateway provides encryption and the use of authentication tokens and credentials with trusted partners. Unfortunately, these measures are required but are not sufficient. Tokens and credentials can be stolen and then used to conduct API-based attacks. Proper API cybersecurity requires multiple layers of protection in order. This is often called "security in depth." These layers are:

- A **perimeter firewall**, such as the Fortinet FortiGate, to prevent DDoS attacks and random connections from unauthorized or untrusted partners.
- A **demilitarized zone (DMZ)**, enforced by a next-generation firewall (NGFW), such as the FortiGate, where the API gateway will be placed to avoid lateral movement across the network in case of a breach.
- A **web application and API protection (WAAP)**, such as the Fortinet FortiWeb, that frontends the API gateway and protects it against a common set of attacks. Machine learning (ML) is advisable to learn and understand APIs' current and evolving behavior so that the API flexibility is not limited.
- An **API gateway**, such as the Fortinet FortiWeb, to control access from partners (with tokens and credentials), will bill the partners and log their activity.
- A **threat intelligence service**, such as Fortinet's FortiGuard Labs, to provide actionable threat intelligence information (such as attack signatures), maintaining the API security infrastructure up to date and effective in the face of evolving threats and attacks.

Optionally, an MNO may decide to add some more layers, such as:

- A **reconnaissance tool**, such as Fortinet FortiRecon, to scan the outer surface to find stranded/shadow assets and APIs and identify potentially vulnerable assets.
- A **monitoring tool**, such as Fortinet FortiMonitor, to report the behavior, performance, and availability of exposed APIs and interfaces.
- A **security information and event management (SIEM) solution**, such as Fortinet FortiSIEM, to process logs, provide event correlation, and flag any unusual behavior.

The diagram below outlines the major layers of cybersecurity in a GSMA Open Gateway context.



Conclusions

The GSMA Open Gateway initiative is an important step in facilitating and streamlining third-party consumption of network capabilities and services, generation value, and revenue for MNOs. The growing implementation of open gateways by MNOs and third parties coupled with the increased use of the exposed APIs by different applications and use cases can only be sustained if the appropriate cybersecurity mechanisms are implemented as part of any open gateway implementation, as outlined in this paper.

Fortinet's Security Fabric platform provides the entire scope of "security in depth" components required to ensure safe and profitable consumption of 5G networks capabilities and services in a fully integrated and automated manner.

[1] GSMA Open Gateway, accessed June 29, 2023.

July 7, 2023 10:31 PM
2245704-0-0-EN