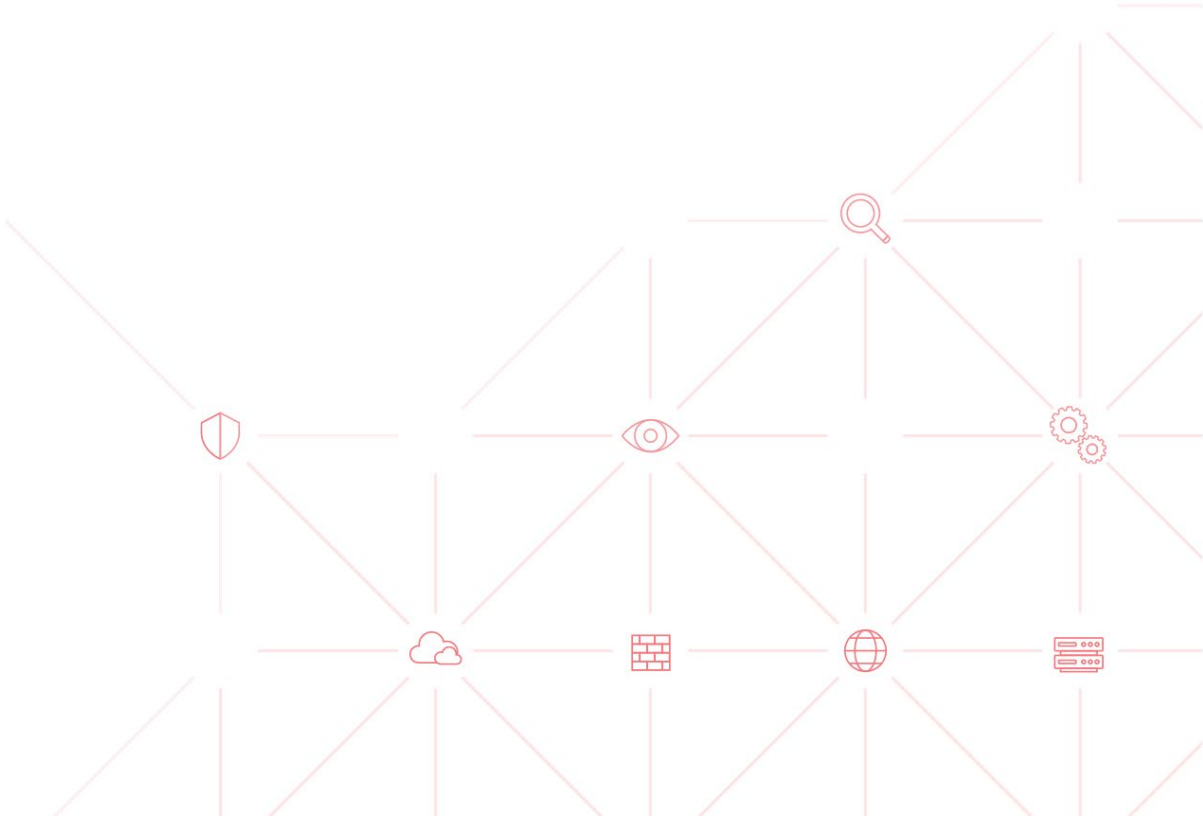
PIOLINK

API 보안과 WAAP(Web Application and API Protection)

API Security White Paper



API 보안 왜 필요할까?

오늘날 개발되는 대부분의 애플리케이션에는 API가 자연스럽게 포함되어 있다. 또한 국내에서는 '22년 1월부터 API 사용을 법적으로 의무화한 마이데이터 서비스까지 시행되었다.(자세한 내용은 앞서 발간한 "WEBFRONT-K API 보안"을 읽어보기 바란다.) 이렇듯 API는 기술에 대한 신뢰성, 보안성, 편의성을 인정받아 빠르게 보편화되고 있다. 그렇다면 실제 API 사용량이 얼마나 되길래 API에 관심을 가져야 한다는 걸까? 아카마이(Akamai)가 발표한 내용에 따르면 최근 아카마이 CDN에서 측정한 트래픽의 80% 이상이 API와 관련된 트래픽이라고 한다.(출처 : 아카마이 엣지 클라우드 보안 전략 웨비나 '22.3.17) 이 데이터만 놓고 본다면 이제는 API를 사용하는 게 특별한 것이 아닌 API를 사용하지 않는 트래픽이 특이한 것이라 봐야 할 것 같다. 이런 사례와 자료들이 보여주듯 API 사용은 이제 웹 환경에서 당연한 것이 되어가고 있다.

1) 안전한 마이데이터 서비스를 위한 API 보안

유관기관(금융위원회, 금융감독원, 금융보안원)과 마이데이터 사업자의 적극적인 참여로 언론에 노출될 정도의 큰 서비스 장애 이슈 없이 마이데이터 서비스가 시행된 지 한 분기가 지났다. (시행일:'22.1.5) 한 분기가 지난 지금 서비스를 시행하고 있는 마이데이터 사업자는 56개 기업('22.4.11 기준)이며, 매달 신규 사업자로 등록되는 기업도 꾸준히 늘고 있다. 이렇듯 마이데이터 서비스를 이용한 시장은 안정적으로 자리를 잡아가며 성장 중이다.

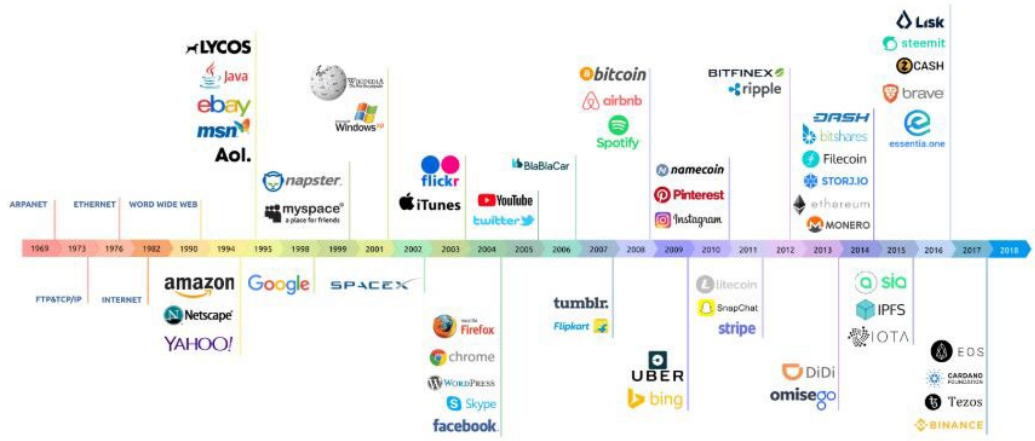
안정적으로 가용성이 확보된 IT 서비스의 다음 과제는 기밀성과 무결성을 확보하는 것이다. 즉 서비스 수준을 유지하면서 보안을 강화해야 하는 단계이다. 특히 마이데이터 서비스는 개인정보를 다루기 때문에 보안에 대한 중요성이 다른 IT 서비스들보다 강조된다. 실제로 '22년 3월 3일 실시한 금융위원장 주관 마이데이터 발전을 위한 간담회에서도 위원장의 모두 발언 및 참석자들의 주요 제안에서 보안 강화에 관한 주제들이 언급되었다.

보안 강화를 위해서는 제도적 보안과 기술적 보안이 필요하다. 제도적 보안은 법적으로 서비스 제공자나 사용자의 부정적인 행위를 제한하거나, 보안을 위한 특정 기술 또는 정책 적용을 의무화하는 보안 개념이다. 마이데이터 서비스를 본다면 "금융분야 마이데이터 기술 가이드라인"에 명시된 보안 조치들을 들 수 있다. 기술적 보안은 보안 사고 예방을 위해 정보보호 장비 도입 등 선제적인 보안 체계를 갖추는 개념이다.

그렇다면 마이데이터 서비스의 보안 강화를 위한 기술적 보안조치는 어떤 것이 있을까? 마이데이터 서비스의 기술적 특징을 생각한다면 가장 강조되는 부분은 역시 API에 대한 보안일 것이다. 실제로 마이데이터 사업자들은 "금융분야 마이데이터 기술 가이드라인"에 명시된 양방향 TLS 등 API와 관련된 보안조치를 시행 중에 있으며 그 밖에도 API 보안을 위한 보안 장비에 관심을 보이고 있다. 물론 아직은 과도한 보안 조치로 인한 서비스 품질 저하 등의 이슈를 우선적으로 고려하여야 하는 시기이기 때문에 선뜻 보안 장비를 도입하긴 어려울 수 있다. 그러나 글로벌 시장의 API 보안에 대한 분위기와 API와 관련된 CVE 취약점 등이 증가하는 것을 고려하면 멀지 않은 시일에 API 보안과 관련해 더 많은 기술들이 제도적으로 요구될 것이다.

2) API 사용이 일반화 되는 미래 웹 환경

NFT, 블록체인, 가상화폐. 해당 키워드들은 작년부터 뉴스, 인터넷, 심지어 관련 도서까지 어디서나 보고 들을 수 있던 기술 용어들이다. 기술들에 대해 하나하나 설명하기에는 해당 백서와 성격이 맞지 않을 수 있지만, 한 가지 말하고 싶은 것은 위의 기술들이 공통적으로 갖는 기술적 특징이다. 위 기술들의 공통점은 바로 탈중앙화 이다. 탈중앙화는 간단히 말하면 데이터를 중앙 서버에 저장하여 관리하는 것이 아닌 각 데이터에 대한 권리를 가지고 있는 기관 및 기업의 서버, 또는 각 클라이언트들이 데이터를 소유하는 개념이다. 즉 특정 기관과 기업에서의 데이터 독점이 아닌 각각의 데이터에 대한 소유권을 인정해 주는 것이다. 사실 이런 개념은 웹이 처음 탄생할 때부터 담고 있던 본질이었다. 월드 와이드 웹의 창시자인 팀 버너스 리(Tim Berners-Lee)는 "웹이 꿈꾸는 세계는 우리가 정보를 공유하고 소통하는 공동의 정보 공간을 만드는 것입니다."라고 말했었다. 결국 팀 버너스 리가 그린 웹 공간은 탈중앙화 기술을 바탕으로 실현되고 있으며, 이런 웹 환경을 두고 우리는 웹 3.0이라는 표현으로 새로운 웹 환경을 준비하고 있다. 물론 웹 3.0에 대해 정의하거나 어떤 모습과 기능으로 우리에게 다가올 것이라 말할 수는 없지만 웹 2.0이 그랬던 것처럼 서서히 우리 곁에 녹아들 것이다.



[그림 1] 웹 생태계 변화 (출처: 해시넷 위키)

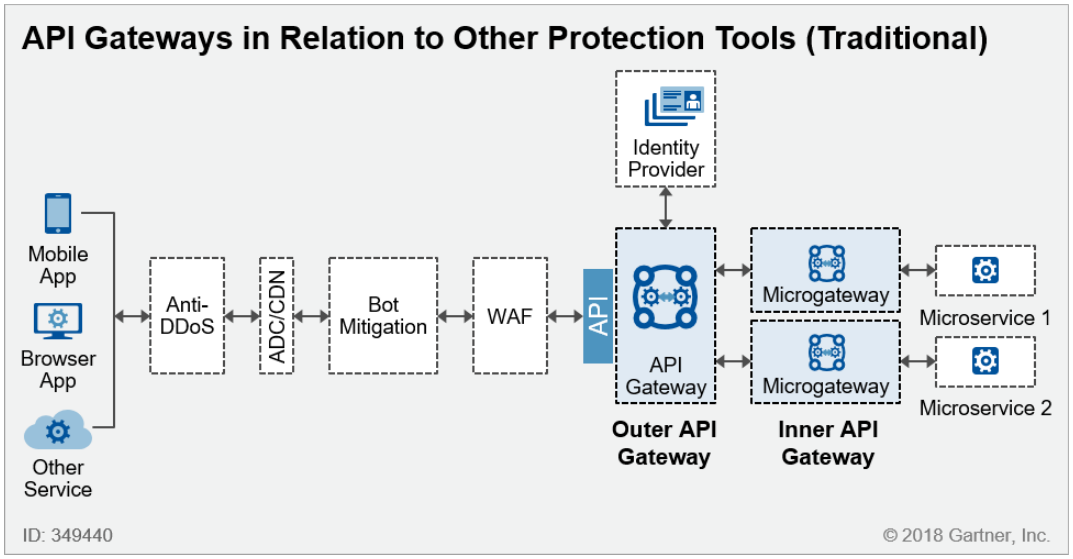
그렇다면 탈중앙화가 API와 어떤 관련이 있는지 살펴보자. 탈중앙화 이전의 환경에서는 필요한 데이터가 있으면 포털사이트에 검색해 해당 포털에 연결된 서버에서 데이터를 가져오는 방법이었다. 하지만 탈중앙화 환경에서는 전용 검색엔진(어떤 형태 일지는 단정지을 수 없다.)을 통해 검색을 하면 분산된 각각의 서버 및 클라이언트들에게 데이터를 요청하고, 요청에 대한 응답으로 해당 데이터를 제공받게 된다. 그리고 이 과정에서 데이터에 대한 요청과 제공이 모두 API로 이뤄지게 된다. 즉 각각의 클라이언트들까지 API를 통한 데이터 공유가 기본인 환경이 되는 것이다. 이미 전세계적으로 본다면 이런 환경은 빠르게 조성 중에 있으며, 이런 환경에서의 위협들도 확인되어 대응책이 마련되고 있는 단계이다. 대표적으로 "WEBFRONT-K API 보안"에서 소개한 "2019 OWASP API TOP10" 취약점을 들 수 있다. 특히 취약점들 중 1, 2, 3번에 해당하는 손상된 개체 수준 권한, 손상된 사용자 인증, 과도한 데이터 노출과 같은 취약점들은 클라이언트와 서버 간의 통신, 클라이언트와 클라이언트 간의 통신에서 주로 발생할 수 있는 취약점이다. 이러한 취약점은 API의 사용이 일반화된 웹 환경을 고려하여 작성된 것이다.

WAAP(Web Application and API Protection)의 등장

- 웹방화벽(WAF)의 진화

최근 API 보안과 관련하여 다양한 정보보호 제품들이 등장하고 있다. 또한 많은 기업들이 이런 API 보안 제품들에 대해 관심을 보이고 도입까지 하고있다. API에 대한 보안을 강화한다는 관점에서 본다면 좋은 시장 분위기이다. 다만 한 가지 의아한 것은 국내 시장에서 인기를 끌고 관심을 받고 있는 대부분의 API 보안 제품들은 글로벌 IT 시장 기준으로 API 관리 시스템으로 구분되는 장비들이다. 물론 보안에 있어 자산을 파악하고 가시화하여 관리하는 것이 중요하기는 하지만 그것은 어디까지나 모니터링 수준의 보안이다. 모니터링은 대부분 내부에서 발생하는 이상에 대해 탐지하고 조치하기 때문에 OWASP에서 정의하는 취약점들처럼 클라이언트나 외부에서 시도하는 위협들에 대한 차단, 또는 정책을 만들어 보안을 강화하는 것과는 다른 개념이다.

그러면 외부로부터 시작되는 API에 대한 위협은 어떤 장비로 대응할 수 있을까? [그림 2]는 글로벌 IT 시장 조사 기업인 가트너(Gartner)가 2018년에 API Gateway에 대해 정의한 그림이다.



[그림 2] API Gateway와 기타 정보보호장비와의 관계 (출처: 가트

그림에서는 Outer API Gateway, Inner API Gateway로 구분하여 내·외부에서 발생하는 API 이슈에 대해 각각의 장비가 관리한다는 개념을 가지고 있다.

하지만 가트너는 다음 해인 2019년에 웹 애플리케이션 보호, DDoS 방어, 봇 관리, API 보호와 같이 4가지 핵심 기능을 갖춘 WAAP(Web Application and API Protection)를 웹방화벽(Web Application Firewall)의 진화된 모델로서 소개하였다.

> Gartner defines web application and API protection (WAAP) as the evolution of the web application firewall market (WAF), expanding WAF capabilities to four core features (see Defining Cloud Web Application and API Protection Services):
>
> - WAF
> - Distributed denial-of-service (DDoS) protection
> - Bot management
> - API protection

[그림 3] WAAP의 4가지 핵심 기능 (출처: 가트너)

그리고 2021년에는 'WAAP 분야 매직 쿼드런트 2021'이라는 웹방화벽 시장 분석 보고서를 대체하는 보고서를 발표하였다. 해당 해에는 웹방화벽에 대한 시장 분석 보고서가 존재하지 않으며, 향후에도 WAAP 보고서로 대체될 것으로 보인다.

결국 [그림 2]의 Anti-DDoS, Bot Mitigation, WAF, Outer API Gateway를 하나로 묶은 개념의 보안장비로 WAAP를 정의한 것이다. 물론 DDoS의 경우 네트워크 계층과 애플리케이션 계층에서 대응이 가능하지만 WAAP에서 말하는 DDoS 대응은 주로 애플리케이션단에서의 대응을 말한다. 사실 이미 대부분의 웹방화벽은 애플리케이션단의 DDoS 대응과 악성 Bot에 대한 대응이 가능하기 때문에 WAAP는 실질적으로 웹방화벽에 API 보안 기능이 추가된 개념이다.

왜 API 보안 기능을 웹방화벽에 추가하였는지는 API의 기술적 특징을 보면 간단히 알 수 있다. 우선 API는 기본적으로 동작 환경이 웹이라는 카테고리 안에 존재한다. 특히 대부분의 API는 HTTP 프로토콜을 기반으로 동작하며, 데이터 전송 형태도 웹 애플리케이션에서 사용하는 JSON이나 XML을 사용한다. 한마디로 API 보안의 기본은 API까지 고려한 웹 애플리케이션 보안을 수행하는 것이다.

이런 기술적인 특징들만 보더라도 API 보안은 웹방화벽에서 구현하는 것이 적절하다. 그리고 이미 대부분의 글로벌 웹방화벽 기업들은 WAAP라는 이름의 장비들과 솔루션을 내놓으며 API 보안을 위한 대표적인 장비로 WAAP 시장을 형성하였다.

하지만 아직 국내 시장에서는 WAAP에 대한 인지도가 낮으며, 아직도 API 보안을 위해 어떠한 장비를 도입해야 하는지 명확한 가이드가 없어 많은 정보보호 담당자들이 어떤 기능이 필요하며 어떤 장비를 도입해야 하는지 정확히 판단하기 힘든 상황이다. 하지만 한 가지 확실한 것은 이미 글로벌 시장에서는 API 보안을 위한 장비로 WAAP를 도입하고 있으며, 그 주요 기능으로는 앞서 가트너가 정의한 4가지 핵심 기술과 OWASP에서 정리한 API 10대 취약점에 대한 대응 기능이 핵심이라는 것이다.

안전한 마이데이터 서비스 구축과 앞으로 다가올 웹 3.0시대를 대비해 API 보안은 필수적인 요소라고 생각된다. 그렇기 때문에 파이오링크는 API 보안에 대해 고민하는 많은 분들께 조금이라도 도움이 되고자 글로벌 트렌드를 분석하고, 다양한 루트를 통해 수집된 정보를 활용하여 보다 나은 API 보안 기술 개발을 위해 연구하고있다. API 보안과 관련한 추가적인 정보를 제공받고 싶은 분들께서는 파이오링크의 API 보안 전문가와 상담해 보길 바란다.(이메일: waf@piolink.com)