대체 불가능 토큰(Non-fungible Token)을 이용한 OAuth 2.0 인증 프로토콜 개선

정혜선, 김경백

전남대학교 정보보안협동과정

Improving the OAuth 2.0 authentication protocol using non-fungible tokens.

HeySeon Jeong, Kyungbaek Kim

Interdisciplinary program of Information Security Chonnam University

요 약

기존의 OAuth 2.0 Refresh Token 인증 방식의 경우 Access Token의 재발급을 위한 Refresh Token이 탈취되는 경우 제 3자가 제약 없이 서비스 사용자의 정보에 접근할 수 있는 문제점이 제시되어왔다.

이 논문에서는 블록 체인 네트워크를 이용하여 토큰 탈취 위험을 개선한 인증 프로토콜에 대해 제안한다. 특히, 소유권을 주장하여 본인임을 인증할 수 있는 대체 불가 토큰(Non-fungible Token; NFT)을 이용하여 인증을 시도하는 계정의 소유자가 본인임을 인증하도록 하여 OAuth2.0 프로토콜의 사용자 인증 흐름을 개선한다.

I. 서론

최근 많은 서비스들에서 사용자 인증을 위해 토큰 기반 인증 방식인 OAuth2.0 프로토콜을 이용해 사용자 인증을 수행한다. 그 중 특히, 만료 시간이 각기 다른 Access Token, Refresh Token 2개의 토큰을 이용하는 방식을 많이 사용한다. 하지만 토큰 자체가 Http 프로토콜의 헤더에 그대로 노출되기 때문에 제 3자에게 쉽게 탈취당할 수 있을 뿐 아니라, Refresh Token까지 탈취 당하면, 토큰을 탈취한 3자는 손쉽게 사용자의 권한을 얻을 수 있다는 문제점이 존재한다. 이 논문에서는 블록체인 기반 기술의 대체 불가능 토큰(Non-fungiable Token)을 이용하여 인증에 사용되는 토큰의 탈취에 대응하기 위한 모델을 제안한다.

II. OAuth 2.0

Web 환경에서의 사용자 인증은 과거 세션기반의 사용자 인증에서 토큰을 이용한 사용자 인증을 많이 사용하는데, OAuth2.0 프로토콜의 Refresh Token 방식을 많이 사용한다.

(그림 1) OAuth 2.0 Refresh Token 방식 인증 프로세스

1. 사용자가 로그인
2. 서버는 정상 사용자인지 여부를 판단한 후, Access Token과 Refresh Token을 전달
3. 사용자는 데이터 요청 시 Access Token과 함께 요청
4. 서버는 Access Token을 확인하여 정상적인 토큰인 경우 응답에 요청 데이터 전달

5. 만료된 Access Token과 함께 사용자가 데이터 요청
6. 만료된 Access Token에 의해 사용자의 요청을 거부
7. 사용자는 새로운 Access Token을 발급받기 위해 로그인 시 발급받은 Refresh Token과 함께 Access Token 재발급 요청
8. 서버는 응답으로 재발급 된 Access Token을 응답으로 전달

이 과정에서 서버는 Access Token으로만 사용자를 판단하고 응답을 전달하며, Refresh Token의 만료 시간은 짧으면 15일에서 길게 30일까지 설정 하기 때문에, Refresh Token이 제3자에게 탈취당할 경우 손쉽게 Access Token을 발급받고 사용자의 정보에 접근할 수 있게 된다.

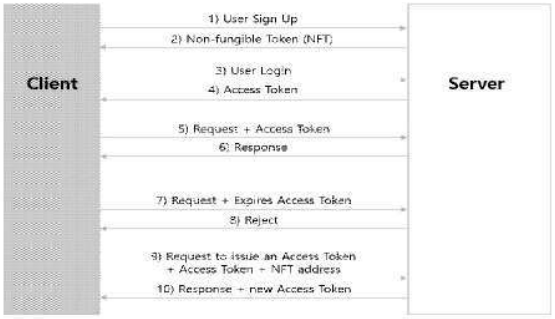
III. 대체 불가 토큰(Non-fungible Token)

NFT는 ERC-721 공개 표준에 명시되어 있는 블록 체인 기반의 토큰으로써 고유한 상태와 값을 가져 발급된 토큰의 가치를 다른 토큰으로 나누거나 대체할 수 없는 토큰을 의미한다. 이러한 특성으로 NFT는 보증서의 개념으로 자주 사용된다.

이 논문 제안하는 인증 프로토콜에서는 NFT의 이러한 특징을 이용하여 사용자 정보 일부를 NFT에 저장, 조회하여 사용자를 특정 짓는데 활용한다.

IV. 대체 불가 토큰을 이용한 OAuth 2.0 인증 개선 모델

대체 불가 토큰을 이용하여 서비스 사용자의 인증과 함께 토큰 탈취의 위험에 대응하는 프로토콜을 개선 모델을 제안한다.



(그림 2) NFT를 이용한 OAuth 2.0 인증 개선 모델

기존의 OAuth2.0 프로토콜 흐름에서 추가/변경 되는 과정은 다음과 같다.

1. 사용자가 서비스에 가입 시 정보(id, service provider)를 바탕으로 서버는 NFT 토큰을 생성하고 이를 사용자에게 전달한다.
2. 사용자는 기존 방식대로 서비스를 이용하며 인증 프로세스를 진행한다.
3. Access Token이 만료가 되면 Refresh Token을 사용하여 재발급 했던 것과 달리, 사용자에게 NFT의 주소를 요청하여 토큰에 기록된 정보를 확인한다.
4. 가입 시 발급했던 정보와 토큰의 정보가 일치하면 새로운 Access Token을 생성하고 사용자에게 전달 한다.

NFT는 블록 체인 네트워크에 저장된 정보의 소유권을 주장할 수 있는 수단으로서 제안하는 모델에서는 회원 가입시 입력한 정보의 일부가 블록 체인 네트워크에 저장되고, 저장된 데이터의 소유권을 나타내는 NFT를 서비스 사용자에게 전달한다.

이후 사용자가 로그인을하고 발급받은Access Token이 만료될 경우, 사용자는 NFT를 서버로 전달하여 정당한 사용자임을 증명하게 되면 서버는 이를 판단하고 Access Token을 재발급해 사용자에게 전달한다.

V. 결론

본 논문에서는 대체 불가능 토큰(NFT)을 이용하여 사용자를 특정할 수 있는 정보를 블록 체인 네트워크에 저장하고 이를 상대적으로 만료 시간이 짧은 Access Token 재발급에 이용함으로써 OAuth2.0 프로토콜에서 취약점으로

제시되었던 Refresh Token 탈취 문제를 해결하는 인증 모델을 제시하였다.

향후 연구로 NFT를 이용한 멀티 플랫폼에서의 사용자 인증에 대한 연구를 진행할 생각이다.

ACKNOWLEGEMENTS

본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 사회맞춤형 산학협력 선도대학(LINC+) 육성사업의 연구결과입니다.
이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (IITP-2019-0-01343)

[참고문헌]

[1] 민경식, 김관영, 박진상, “KISA Insight Vol 3.0 NFT 기술의 이해와 활용, 한계점 분석”, 2021. 09.

[2] “OAuth 2.0”, https://oauth.net/2/, (Accessed: 07 Octobor 2021.)

[3] “Klaytn API Documents”, https://docs.klaytnapi.com/”, (Accessed: 07 Octobor 2021.)

[4] “OAuth 2.0 Framework RFC 6789”, “https://datatracker.ietf.org/doc/html/rfc6749#section-1.7”, (Accessed: 07 Octobor 2021.)

[5] “ERC 721 documents”, https://docs.openzeppelin.com/contracts/3.x/erc721, (Accessed: 07 Octobor 2021.)