Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Porovnanie API tokenov

Bakalárska práca

2023
Jitka Muravská

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Porovnanie API tokenov

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	RNDr. Richard Ostertág, PhD.

Bratislava, 2023
Jitka Muravská

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Jitka Muravská
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Porovnanie API tokenov
Comparison of API Tokens

Anotácia: REST aplikačné rozhrania (API) často nebývajú čisto verejné. V takom prípade treba pri implementácii API riešiť aj jeho bezpečnosť. Väčšina schém zabezpečenia API používa token, ktorý je súčasťou jednotlivých požiadaviek. Tieto tokeny sú nejakým spôsobom spojené s identitou a autorizáciou používateľa. Aplikačné rozhranie prevezme požiadavku, extrahuje token, a podľa pravidiel prístupu rozhodne ako pokračovať.

Cieľom práce je porovnanie rôznych API tokenov (napríklad: OAuth 2.0, JWT, PASETO, Protobuf Tokens, Authenticated Requests, Macaroons, Biscuits, …). Prvým krokom bude zozbieranie a popísanie rôznych v praxi používaných API tokenov. Následne sa vykonajú porovnania ich výhod a nevýhod (napríklad rýchlosť, jednoduchosť použitia) na jednoduchej základnej aplikácii.

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 12.10.2022

Dátum schválenia: 13.10.2022 doc. RNDr. Dana Pardubská, CSc.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie:

Abstrakt

Kľúčové slová:

Abstract

Keywords:

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Kapitola 1

Prehľad a súvisiaca literatúra

V tejto kapitole sa zameriame na prehľad témy API tokenov a súvisiacu literatúru, ktorá sa venuje nami skúmanej problematike. Popíšeme, čomu sa nižšie uvedené zdroje venujú a ako sa líšia od cieľov našej práce.

1.1 Prehľad

Ako prvé si v krátkosti predstavíme tému API tokenov a vysvetlíme základné pojmy. API token (ďalej token) je identifikátor, ktorý sa používa na autorizáciu prípadne aj identifikáciu používateľa pri prístupe k API. Používateľom v tomto kontexte môže byť webová aplikácia, server alebo iný program, ďalej ich súhrnne budeme označovať ako klient.

Token typicky vydáva autentifikačný server danej API, voči ktorému sa klient autentifikuje, zväčša prihlasovacím menom a heslom. Následne autentifikačný server vytvorí token pre klienta a tento token bude používať klient pri ďalších požiadavkách na API. Token je typicky uložený v pamäti klienta a pri každej požiadavke na API je posielaný spolu s inými údajmi. Tokeny sa môžu vytvárať pomocou šifrovania, elektronických podpisov alebo hešovania.

1.2 Súvisiaca literatúra

K problematike rôznych typov tokenov nie sú dostupné odborné články alebo knihy a odborná literatúra spočíva najmä z príspevkov na blogoch a technických špecifikácií autentifikačných a autorizačných protokolov a konkrétnych tokenov. Zamerali sme sa na blog zachytávajúci najširší záber tokenov.

1.3 Porovnanie do šírky

Tokeny sa môžu líšiť štrukturálne. To znamená, ktorou dátovou štruktúrou sú reprezentované a akú informáciu v sebe nesú. Obyčajne takto delíme tokeny na nepriehľadné (angl. opaque) a štruktúrované. Nepriehľadný token predstavuje náhodný reťazec, ktorý neobsahuje (ani v zašifrovanej podobe) relevantnú informáciu, naopak štruktúrovaný token obsahuje navyše informáciu vhodnú pre API, napríklad môže obsahovať identifikátor používateľa, pre ktorého bol vydaný, čas vytvorenia alebo dátum exspirácie.

Širokospektrálnemu prehľadu hlavne štruktúrovaných typov tokenov sa venuje na svojom blogu [2] Thomas Ptacek. V texte najprv uvádza najjednoduchší typ tokenu a to nepriehľadný token pozostávajúci z náhodného reťazca a označuje ho ako náhodný token. Náhodný token je výhodný, lebo na jeho vydanie ani overenie netreba počítať zložité kryptografické funkcie. Jednoducho sa vygeneruje náhodný reťazec. Problém náhodných tokenov je, že si API potrebuje udržiavať zoznam aktívnych tokenov a im zodpovedajúcich metadát ako napríklad používateľa, pre ktorého bol token vydaný, ku ktorým volaniam má daný používateľ prístup, či časovú pečiatku dokedy je token platný.

Neskôr prechádza postupne viacero typov tokenov ako JSON web token (JWT), PASETO, CAT (z anglického Crypto Auth Token) a makaróny (angl. macaroons). O každom sa dozvieme ako je daný token reprezentovaný a ďalej sa autor venuje hlavne kryptografickej bezpečnosti. Autor pomyselne rozdelí tokeny na *podobné JWT* a *Anti-JWT*.

1.3.1 podobné JWT

Tu sa zameriava na porovnanie JWT a POSETO. Oba sú štruktúrované a kým JWT, ako z názvu vyplýva, je reprezentovaný štruktúrou JSON, PASETO môže byť v niektorých verziách zachytený aj štruktúrou CBOR (z anglického Concise Binary Object Representation). Ptacek hlavne rozvíja problémy JWT, ktorý označuje za *kryptografický neporiadok*. JWT dovoľuje programátorovi si vybrať kryptografické zabezpečenie z veľa rôznych symetrických aj asymetrických riešení. Týmto sa otvárajú dvere bezpečnostným zraniteľnostiam. Napríklad problém známy ako RSAtoHMAC [1] využíva fakt, že pri verifikovaní nechávame útočníka si vybrať, ktorá metóda sa používa na verifikáciu tokenu.

Problémy, ktoré má JWT sa snaží vyriešiť PASETO. Verzionuje celý protokol a nepridáva nové možnosti pre programátora v rámci jednej verzie, čím sa snaží vyvarovať spomínanému *kryptografickému neporiadku*. Najväčší problém PASETO, ktorý autor vypichuje je viacero aktuálnych verzii. PASETO má spolu 8 verzii, z ktorých až 4 sú

označené za aktuálne.

Záverom jeho pozorovaní je, že je lepšie použiť PASETO, ale stále to nie je ideálne riešenie a je silno naklonený k použitiu *Anti-JWT* tokenov.

1.3.2 Anti-JWT

Anti-JWT tokeny sú tokeny, ktoré odstraňujú problémy JWT, lebo nepoužívajú podpisy ani zdieľané tajomstvo medzi API, autentifikačným serverom ani klientom. Autor uvádza CAT a makaróny. Obe tieto riešenia fungujú na základe *zlatého kľúča*, ktorý pozná len autentifikačný server. Z neho odvádza overovací kľúč pre API, z ktorého ďalej vytvorí konštrukčný kľúč pre klienta. Klient si následne pomocou svojho kľúča vytvorí token, ktorý použije na prístup k API. API vie tento token overiť, lebo je vytvorený známym spôsobom z overovacieho kľúča, ktorý pozná.

Pri týchto protokoloch najviac vyzdvihuje flexibilnosť, jednoduchosť a najmä *kryptografický poriadok*, ktorý prinášajú. Kedy je jasné ktorý algoritmus sa používa na kryptografické zabezpečenie.

1.3.3 V čom je naše práca iná

Ptacek sa vo svojom blogu venuje hlavne kryptografickej bezpečnosti tokenov. A celkovo robí prehľad najmä do šírky a nevenuje sa detailom jednotlivých protokolov. V našej práci chceme porovnávať tokeny podľa viacerých kritérií, teda spraviť komplexnejšie porovnanie. Tokeny budeme samozrejme porovnávať aj podľa bezpečnosti, keďže to je ich dôležitý aspekt. No navyše porovnáme aj ich flexibilnosť, škálovateľnosť, jednoduchosť, rýchlosť a ďalšie kritériá.

Kapitola 2

Využitie API tokenov

V tejto kapitole si priblížime, kde sa využívajú API tokeny a aké sú rozdiely pri použití tokenov v autentifikačnej a autorizačnej schéme oproti iným známym prístupom ako API kľúče, či využitie prihlasovacieho mena a hesla.

Kapitola 3

Typy API tokenov

V tejto kapitole predstavíme v praxi využívané typy API tokenov a uvedieme ich základné charakteristiky.

Kapitola 4

Teoretické parametre API tokenov

V tejto kapitole porovnáme teoretické parametre rôznych typov API tokenov ako bezpečnosť, škálovateľnosť a flexibilita.

Kapitola 5

Praktické parametre API tokenov

V tejto kapitole porovnáme praktické parametre rôznych typov API tokenov ako jednoduchosť implementácie a rýchlosť.

Kapitola 6

Porovnanie na jednoduchom rozhraní

V tejto kapitole navrhneme a implementujeme jednoduché rozhranie s použitím viacerých typov API tokenov. Výsledkom budú naše pozorovania pri implementácii a použití rozhrania s jednotlivými typmi API tokenov.

Záver

Literatúra

[1] Tim McLean. Critical vulnerabilities in json web token libraries, August 2020. https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/.

[2] Thomas Ptacek. Api tokens: A tedious survey, August 2021. https://fly.io/blog/api-tokens-a-tedious-survey/.