Prihlasovanie do GateIn Portálu

pomocou účtov facebook, google a twitter

Bc. Matej Kobza Brno 2012 Czech Republic **T** 0949 464 715 matej.kobza@gmail.com

Možnosti prihlasovania

Našou snahou je do portálu GateIn pridať možnosť prihlasovania pre užívateľov, ktorý si nechcú registrovať a vytvárať nový prihlasovací účet, cez ktorý by do portálu pristupovali, ale radšej chcú použiť niektorí z účtov, ktoré už majú k dispozícii na inom mieste v internete. Typickým príkladom by bolo použitie účtu zo sociálnych služieb ako Facebook, Google+ či Twitter. Tieto služby by tak boli poskytovateľom identity prihlaseného uživateľa.

Pohľady poskytovateľov identít (berieme do úvahy Facebook, Google a Twitter) sa už typicky líšia a nájsť tak najvhodnejšie riešenie nie je úplne jednoduché. Môžme však nájsť jednoduchý vzor, ktorý je vo všeobecnosti braný ako správny prístup k danej problematike. Za základný kameň môžme pokladať pravidlo, vždy udržiavať informáciu o prihlasovaciom mene a hesle užívateľa iba na jednom mieste. Tým je poskytovateľ identity. Preto je nevyhnutné vytvoriť nejaký komunikačný kanál, cez ktorý by daná aplikácia tretej strany získala dočasné, obmedzené oprávnenia na prítup k informáciám o prihlasovanom užívateľovi. Prihlasovanie teda vždy prebieha u poskytovateľa identity a taktiež na tejto strane komunikácie dostáva prihlasovaný užívateľ informáciu o tom, k akým zdrojom bude aplikácia ktorú autorizuje mať prístup. Tento princíp si môžme jednoducho vysvetliť na takzvanom peňaženkovom kľúči, ktorý je typicky využívaný v západnom svete pri drahých automobiloch. Predstavme si situáciu, kedy majiteľ luxusného automobilového vozidla ide na spoločenskú udalosť. Pri vstupných dverách odovzdá svoje auto personálu, ktorý ho má za úlohu zaparkovať na príslušnom parkovisku. Obsluhe ale nedá svoj originálny kľúč od vozidla iba takzvaný peňaženkový kľúč, s ktorým je možné odviesť automobil do vzdialenosti maximálne niekoľko kilometrov od originálneho kľúča vozidla. V prípade, že personál presiahne povolenú vzdialenosť, automobil vypne motor a zablokuje sa. Tento prístup je vhodný najmä preto, že potenciálne nedôveryhodnému zdroju poskytujeme len obmedzené oprávnenia a obmedzené množstvo informácii, ktoré nie je tak jednoduché zneužiť. Rovnako aj pri snahe aplikácie o získanie väčších oprávnení, ako dostala pri inicializácii komunikácie s poskytovateľom identity a poskytnutí oprávnení bude tejto aplikácii odopretý prístup vždy keď presiahne svoje kompetencie. Už v minulosti bola snaha o implementáciu tohoto vzoru, a tak bol vytvorený jednoduchý protokol poskytovania identity, všeobecne známy ako OpenID. Jeho bližší popis uvedieme v texte neskôr.

Cieľom tejto správy je poskytnúť uceľený náhľad do možností, ktoré pre tento prístup v dnešnej dobe máme a vybranie najvhodnejšieho riešenia, ktoré bude neskôr v druhej fáze implementované do portálu GateIn.

1. Pomocou prihlasovacieho mena a hesla

Voľbou tohoto riešenia by sme museli pre každý typ učtu na internete pripravovať zvlášť prihlasovací formulár a celý tok dát medzi poskytovateľom identity a portálom pre každého poskytovateľa dotvárať. Naviac, nevýhodou takéhoto riešenia je možný únik prihlasovacieho mena a hesla u poskytovateľa, ktoré je následne možné zneužiť pre prístup údajov v portáli. Toto samozrejme platí aj naopak, nakoľko prihlasovacie meno a heslo musí byť uložené na oboch stranách ako u poskytovateľa tak u príjemcu, ktorý žiada o overenie identity.

2. Pomocou poskytovateľa identity

Tento princíp prihlasovania je preferovaný už niekoľko rokov a je snaha o jeho zdokonalovanie, aby vívojári mali pocit, že ho môžu bezpečne používať. Je založený na vyššie uvedenom princípe a má niekoľko rôznych implementácii:

- OpenID,
- OpenSocial,

- OAuth;

a rôzne ich modifikácie či rozšírené verzie ako:

- OpenID Attribute Exchange,
- OAuth WRAP,
- Google Friend Connect,
- Facebook Friend Connect,
- Facebook Platform,
- Facebook Connect,
- Portable Contacts;

2.1 OpenID

OpenID je decentralizovaný autentizačný protokol, ktorý zjednodušuje uživateľom možnosť prihlásenia a získania prístupu k roznym službám na internete. Definuje akýsi štandard alebo vzor, pomocou ktorého sa je možné preukázať, že sme tým, kým tvrdíme, že sme. Užívatelia, ktorí používajú túto službu si vyžiadajú unikátny identifikátor (typicky nejakú URL) od OpenID poskytovateľa. O tomto identifikátore môžme uvažovať ako o prihlasovaciom mene uživateľa, ktoré je použiteľné kdekoľvek. Ak sa chcete autentizovať ako tento uživateľ (dokázať, že ste vlastníkom spomínanej URL), prihlásite sa k svojmu OpenID poskytovateľovi namiesto toho, aby ste sa prihlasovali do aplikácie, ktorá používa OpenID. Základy OpenID siahajú niekde do doby služby LiveJournal, ktorá chcela dosiahnúť, aby bolo možné používať jednu identitu pre zanechávanie komentárov v ľubovoľnom blogu.

Pre jednoduchosť si skúsme uviesť príklad prihlásenia užívateľa do služby StackOverflow pomocou OpenID:

- Na stránkach služby StackOverflow poskytneme OpenID URL ako prihlasovacie meno.
- StackOverflow kontaktuje Google aby vytvorilo zdielany tajný kľúč[1].
- Prihlásime sa do Google a získame správu podpísanú zdieľaným tajným kľúčom (zvyčajne používa HMAC-SHA256).
- Túto správu poskytneme StackOverflow aby sme dokázali, že sa nám podarilo úspešne príhlásiť.

Toto je prvý spôsob, ktorý definuje OpenID protokol. Požaduje, aby si naša aplikáciu pamatala zdielaný tajný kľúč (musí byť statefull). Avšak OpenID nám dovoluje pristupovať aj iným spôsobom a to nasledovne:

- Poskytneme Google našu OpenID URL.
- Prihlásime sa do Google a budeme informovat StackOverflow o tom, že sa nám prihlásiť podarilo.
- StackOverflow bude potom kontaktovať Google aby si overilo, že sme sa skutočne prihlásili.

V konečnom dôsledku, bezpečnostní výzkumníci vzniesli námietku ohľadom OpenID pre náchilnosť k phishing útokom. Za normálnych okolností tzv. phishing stránka musí oklamať návštevníka, aby navštívil nepravú prihlasovaciu stránku, avšak pri OpenID užívateľ očakáva, že bude automaticky presmerovaný na správnu prihlasovaciu stránku OpenID poskytovateľa.

> *In the standard case, I (the phisher) have to make my website look like the Real Website and persuade you to go to it somehow – i.e. con you into thinking I am the real Paypal, and your account really has been frozen (or is that phrozen?) and you really do need to log in to unphreeze it.*

> *But in the OpenID case I just persuade you to go anywhere at all, say my lovely site of kitten photos, and get you to log in using your OpenID. Following the protocol, I find out where your provider is (i.e. the site you log in to to prove you really own that OpenID), but instead of sending you there (because, yes, OpenID works by having the site you're logging in to send you to your provider) I send you to my fake provider, which then just proxies the real*

provider, stealing your login as it does. I don't have to persuade you that I'm anything special, just someone who wants you to use OpenID, as the designers hope will become commonplace, and I don't have to know your provider in advance.

OpenID je jednou z možností vytvorenia prihlasovania pomocou Google+ účtov do portálu GateIn. Avšak pre nemožnosť implementácie prihlasovania pomocou účtov Facebook či Twitter s ňou nie je možné počítať ako štandardom. Rovnako OpenID neposkytuje možnosť priameho načítania údajov z účtu Google, ktoré je potrebné pre plynulý chod portálu. Z týchto dôvodov sme sa rozhodli poobzerať aj po ďalších možnostiach.

2. OpenSocial

Tomuto štandardu sa budeme venovať len stručne. Jedná sa o štandardizované API pre sociálne siete. Tento štandard bol vytvorený spoločnosťou Google. V skutočnosti sa jedná o dve API. Jedno pre JavaScript a druhé pre REST. JavaScript API slúži pre aplikácie ktoré sú takzvaného typu "web gadgets" písané v architektúre Google gadgetov. REST API slúži pre všetky ostatné typy aplikácií ako desktop, mobilné či serverové. Na pozadí musí každá sociálna sieť podporovať SPI (service provider interface), ktoré poskytuje možnosti ako:

- Pridávanie alebo odoberanie priateľov,
- pridávanie alebo odoberanie aplikácií,
- ukladanie aktivít uživateľa a tak ďalej;

Takzvané "gadgety" sú vždy vytvorené pomocou API[8]. Každá sociálna sieť, ktorá je schopná spustiť OpenSocial "gadgety" je jedným veľkým kontajnérom. Apache Shinding[9] je typickou implementáciou kontajnéru. V skutočnosti "gadget" je JavaScript objekt, ktorý implementuje rozhranie OpenSocial. Autentizácia je mimo rozsahu OpenSocial specifikácie gadgetov a očakáva sa, že bude prevedená v čase, kedy dôjde k inštanciácii gadgetu. Pri JavaScript gadgetoch ju zabezpečuje implementácia OpenSocial kontajnéru a pri REST API je použité typicky OAuth.

3. OAuth (Open Authorization)

OAuth talks about getting users to grant access while OpenID talks about making sure the users are really who they say they are.

Jedná sa o štandard, ktorý vznikol z úsilia spoločnosti Twitter. Snahou bolo poskytnúť uživateľom možnosť ako darovať alebo odobrať prístup aplikáciam tretích strán k ich vlastnému účtu na twitter-i. Namiesto toho, aby uživateľ poskytoval svoje prihlasovacie meno a heslo, čo vedie k neobmedzenému prístupu k účtu, stačí ak uživateľ poskytne tzv. "OAuth tokens", ktoré slúžia pre prístup k specifickému množstvu údajov spojených s daným účtom po presne stanovený čas. Napríklad, užívateľ smie službe TwitterFeed poskytnúť oprávnenie zasielať takzvané tweets na jeho Twitter účet po určitý čas. Keď tento čas uplynie, aplikácia bude pri snahe o zaslanie nového tweetu opäť žiadať oprávnenie pre prístup k danému účtu.

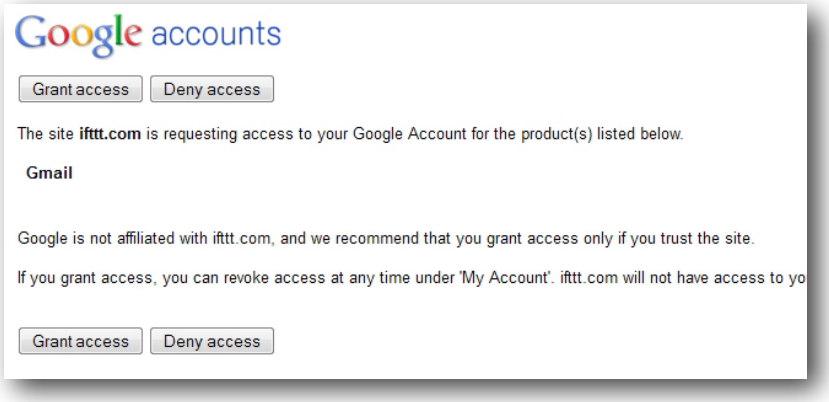
V súčasnosti je tento štandard vo verzii 2.0 avšak tá ešte nie je úplne popísaná a oficiálne vydaná. Z tohoto dôvodu sa niektorí poskytovatelia identít rozhodli zostať ešte stále pri verzii 1.0a, prípadne 1.0.

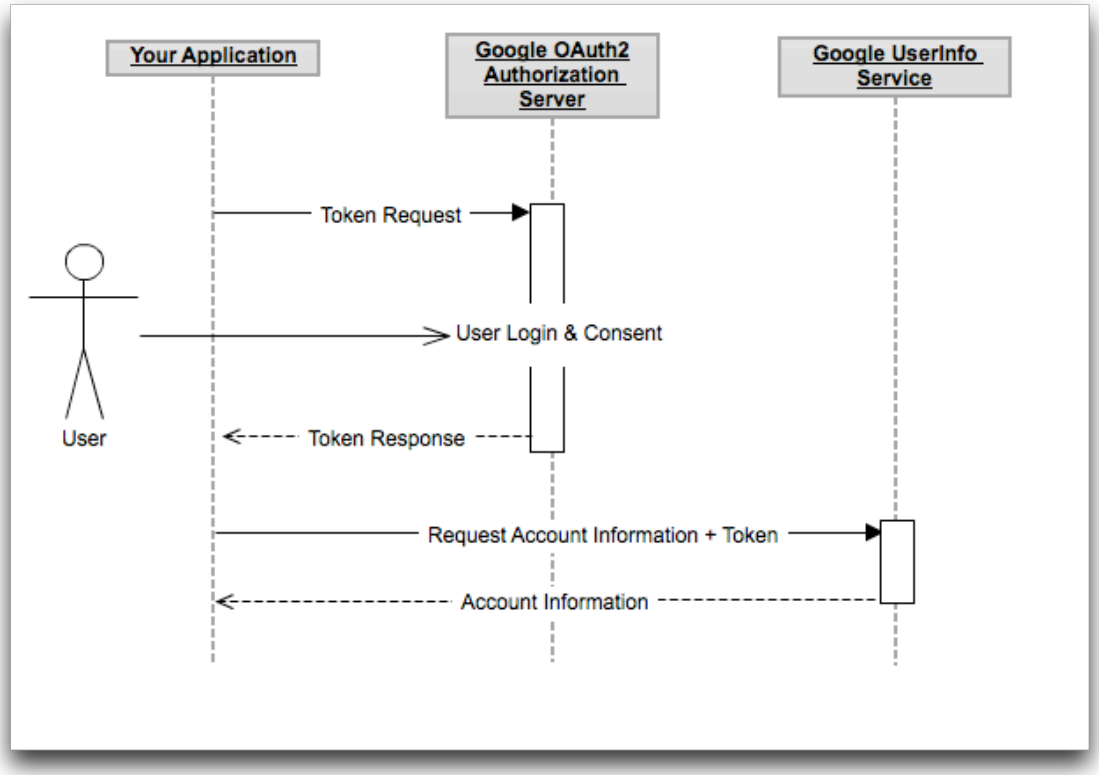
Aký je rozdiel medzi OAuth a OpenID?

Odpoveď na túto otázku je možné nájsť už pod nadpisom. Zásadným rozdielom však zostáva, že pomocou OAuth je možné nie len užívateľa autentizovať ale v skutočnosti aj pristupovať k jeho dátam, informáciám o jeho účte, ktoré sú uložené u poskytovateľa identity. Pomocou OpenID iba získavame informáciu o "pravosti žiadateľa prístupu".

Ako OAuth vlastne funguje?

Na stránkach Lifehacker.com môžme nájsť popis o tom, čo sa deje počas procesu prihlasovania uživateľa pomocou protokolu OAuth. Pojednáva o tom, že prihlásenie pomocou existujúceho účtu na facebooku, google či twitteri je dokonca bezpečnejšie než vytvorenie nového účtu. Pre zjednodušenie uvedieme len hlavnú myšlienku celého procesu prihlásenia a darovania oprávnení aplikácii tretej strany. Na začiatku celého procesu je nevyhnutné, aby aplikácia tretej strany mala priradené dva údaje. Tými sú "Consumer Key" a "Consumer Secret". Tieto určujú kto sa s kým snaží spojiť. Obyčajne je ich možné získať dlhodobo zaregistrovaním aplikácie tretej strany u poskytovateľa identít. Ak navštívime aplikáciu tretej strany a zvolíme si spôsobom prihlásenia pomocou poskytovateľa identít, budeme presmerovaní na stránky poskytovateľa identity, kde vyplníme svoje prihlasovacie meno a heslo. Poskytujeme teda svoje prihlasovacie údaje poskytovateľovi identity a nie aplikácii tretej strany. Po úspešnom prihlásení prichádza otázka, či chceme danú aplikáciu autorizovať[obr 1]. Získavame informáciu o tom, o aké oprávnenia má záujem. Po schválení prístupu sme presmerovaní späť do aplikácie tretej strany, ktorá takto získala oprávnenia prístupu k údajom vašeho účtu. Tieto oprávnenia sú však obmedzené. V preklade si to môžme predstaviť tak, že namiesto toho, aby sme cudzej osobe podarovali kľúč od celého domu, sme jej dali do ruky kľúč, ktorým je možné odomknúť jednu izbu domu, do ktorej chceme aby mala prístup. A ešte vždy musí ísť po tento kľúč k strážcovi domu tesne pred tým, ako chce do izby vôjsť. Celý proces prihlasovania je možné vidieť na obrázku[obr 2].





[1] http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

[2] http://yz.mit.edu/wp/making-sense-of-openid-oauth-opensocial-google-friend-connect-facebook-connect-and-more/

[3] http://oauth.net/about/

[4] http://hueniverse.com/2007/09/explaining-oauth/

[5] http://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook

[6] http://waxy.org/2012/02/the_perpetual_invisible_window_into_your_gmail_inbox/

[7] http://www.optimumclick.com/use-oauth-to-login-your-web-site-with-facebook-google-or-yahoo-accounts/

[8] https://developers.google.com/gadgets/

[9] http://shindig.apache.org

[10] http://openid.net/developers/