

OpenID: Webová vstupenka

Konec heslům! Použijte **KONTO PRO VŠECHNY SLUŽBY**. Chip vám představí OpenID a prozradí vám, jak funguje a jaká má rizika.

VRATISLAV KLEGA

Už jste někdy zapomněli heslo? Pravděpodobně ano. To už se asi stalo každému. A pamatujete si, na kolika webových fórech, blozích, komunitách a portálech jste registrovaní? Asi jen těžko. Přesto byste si měli ke každé službě pamatovat přihlašovací údaje – jméno a heslo. To je děsivé. Řešení je však jednoduché.

Cestou ven je OpenID. Služba je založena na URL a slouží k identifikaci uživatele. Jakmile budete mít OpenID, už si nebudete muset pamatovat přihlašovací údaje ke Googlu, Yahoo nebo Seznamu.

Všude zalogovaný: Průkaz pro všechny stránky

Princip je velmi jednoduchý: OpenID je webový průkaz totožnosti, pomocí něhož se můžete identifikovat na webových stránkách, které OpenID podporují. Aby to fungovalo, musíte si nejprve zřídit konto u OpenID providera. Do něj vyplníte základní údaje, jako je jméno, přezdívka a e-mailová adresa. Na základě těchto údajů se vám vygeneruje internetová adresa, například ve tvaru `http://jmeno.myopenid.com`.

Jakmile si uživatel jednou OpenID zaregistruje a přidá si službu, která OpenID podporuje, již nebude muset zadávat

uživatelské jméno a heslo. Místo uživatelského jména a hesla zadá jen svou doménu (viz výše), a tím se přihlásí ke službě. OpenID pak službě zašifrovaným kanálem předá uživatelské jméno a heslo a dojde k přihlášení. Zadat jméno a heslo stačí jen poprvé, pak už je můžete zapomenout a nechat ve správě OpenID. Výhodou je, že ať už jste kdekoliv, stačí si pamatovat jen svoji URL. Nemusíte s sebou nosit žádného správce hesel a OpenID bude fungovat na všech počítačích, ve všech operačních systémech a v každém prohlížeči. Zajímavé je na této službě to, že už se nepoužívá kombinace jméno+heslo, ale pouze jedina URL adresa. Tento systém se nazývá Single-Sign-on-System (SSO).

Jednoduché ovládání: Automatické doplňování

Jaká data OpenID provider předává službě využívající OpenID, to záleží na použitém profilu. OpenID konta mohou být jak soukromá, tak veřejná. Můžete tedy sdílet e-mailové adresy, fotografie, telefonní čísla i jakékoliv další položky, které jsou v profilu k dispozici. Přihlašujete-li se na webové fórum, bude úplně stačit přezdívka a e-mail, používáte-li blog, nejspíš zveřejníte i nějakou fotografii a svoji WWW stránku.

Komu by se nelíbilo, že pro přihlášení používá tvar `http://jmeno.myopenid.com`, může samozřej-



Přehled historie: MyOpenID.com umožňuje procházet historii činností. Vidíte tak poslední přihlášení i manipulaci s účtem.

mě použít i svoji vlastní HTML stránku na doméně, kterou vlastní. Stačí jen do HTML hlavičky zadat několik tagů s informací o OpenID. Takový systém přihlašování může být zajímavý třeba pro firemní stránky nebo velké množství uživatelů. Teoreticky bychom se v redakci všichni mohli přihlašovat zadáním `http://chip.cz`.

Díky plug-inu OpenID Attribute Exchange (Microsoft podporuje OpenID) je možné do OpenID doplnit veškeré další údaje, a to zcela automaticky. Navíc se všechny informace budou udržovat aktuální, protože bude docházet k automatické synchronizaci s Exchange serverem.

Kdo nechce dát svoje data a údaje z ruky, ten si samozřejmě může postavit svůj vlastní OpenID server. Data má pak uložena zde. Navíc je to velmi jednoduché – server si můžete postavit i bez znalosti programovacího jazyka. OpenID je otevřený a decentralizovaný systém, k dispozici jsou hotové skripty a nástroje. Nechybí ani phpMyOpenID, který stačí jen rozpakovat na webové stránky a spustit. Výhoda: Uživatel nikomu nedává z ruky svoje údaje, všechna hesla zůstávají

Poskytovatelé OpenID

Tyto webové služby nabízejí bezplatné vytvoření konta:

Uzavření providerů
www.microsoft.com
www.google.com
www.yahoo.com

Otevření providerů
www.myopenid.com
<https://pip.verisignlabs.com>
<http://clavid.ch>

OpenID logo: Stále více webových služeb používá jednoduchý způsob přihlášení.

u něj. Bude tak stačit, pokud má zajištěnu bezpečnost svého serveru.

Implementace není vůbec složitá a uživatelé mohou použít hotové knihovny, které jsou dostupné v mnoha programovacích jazycích, včetně Javy, PHP, Pythonu a Perlu. Právě velmi jednoduchý přechod na OpenID a jeho snadná správa dávají systémům SSO šanci na rychlé uchycení.

Aby byly dodrženy všechny standardy OpenID protokolu, kontroluje od roku 2007 organizace stojící za OpenID techniky vývoje. Členem organizace jsou firmy jako Microsoft, Google, Yahoo, IBM, Facebook, MySpace a VeriSign.

Slabá místa: Phishing a krádeže identity

Otevřený protokol nepřináší jen výhody, ale také nebezpečí. Uživatel by měl používat jen takové OpenID providery, u kterých bude mít jistotu, že nezneužijí jeho data a identitu. Jednomu subjektu vlastně svěříte všechna svoje hesla. Navíc nehrozí jen zneužití samotným providerelem, ale i to, že databáze

poskytovatele bude napadena hackerem. V rámečku vlevo dole jsme pro vás vybrali několik poskytovatelů, kteří jsou již prověřeni tisíci uživateli.

Další problém: OpenID je neplacená služba, a není tedy nijak zaručeno, že servery poskytovatele budou v provozu. Pak se budete chtít přihlásit, ale bude to marné – server vás nebude moci ověřit a vy se nedostanete nikam, kam se přihlašujete pomocí OpenID.

OpenID je samozřejmě také velmi citlivé na phishing. Může se stát, že omylem zadáte svoje OpenID na server hackera a ten pak získá vaše údaje. Další problém je v přenosu OpenID. Když jej zadáváte, přenáší se nešifrovaně, takže stačí hacknutý proxy server a hacker má opět v ruce vaše jména a hesla.

Ochranu před phishingem by měl každý čtenář Chipu zvládnout. Jednoduše stačí dávat pozor, na jakých jste stránkách a především doméně. Směšné pro čtenáře Chipu jsou jistě také jakékoliv maily, kde kdokoliv chce, abyste zadali svoje heslo, i když to vypadá, že se jedná o správce účtu. Žádná internetová služba takové funkce nevyžaduje, přesto mají útočníci s tímto typem útoku značný úspěch. Další možností, jak se bránit zneužití, je používání šifrovaného připojení HTTPS.

První experimenty: Google a další sází na OpenID

Webové giganty jako Google, Microsoft a Yahoo vidí v Single-Sign-on-Systemu budoucí standard pro přihlašování ke službám. Také proto jsou samy OpenID providery a doufají ve větší rozšíření. Jenže právě velcí providéři vlastně nevědí, jak s OpenID zacházet. Jsou

totiž jak producenty, tak konzumenty OpenID – nabízejí OpenID účty a využívají jejich služby, což je poněkud paradoxní. Další zvláštností je, že pro přihlášení na Yahoo budete moci využít OpenID, které máte z Googlu. To se jistě přestane velikánům po nějakém čase líbit. Je tedy možné, že OpenID nebude tak kompatibilní, jak se při jeho návrhu počítalo.

I další webové služby znesnadňují OpenID život. Facebook sice podporuje OpenID, ale místo toho, aby se všechna data z OpenID načetla, je třeba provést normální registraci. Přitom právě otravnou registraci, kde se zadává e-mail a další podrobnosti, by mělo OpenID řešit místo uživatele.

OpenID je stále experimentem a čeká se, zda se vůbec uchytí. Nápad je to jistě zajímavý, vyřešil by potíže s pamatováním si hesel, máme však zdvižený prst nad jeho bezpečností. Zde vidíme značné nedostatky. ❌

VRATISLAV.KLEGA@CHIP.CZ

ZÁVĚR

OpenID má řadu výhod: jediným kontem můžete přistupovat ke všem službám na internetu a nemusíte si pamatovat vůbec žádná hesla. Stačí jediná URL adresa, která zná vaši kompletní identitu. Otázkou je nasazení. U nás podporuje OpenID Seznam a několik menších projektů, celosvětově jej podporuje Google a Microsoft, ale ještě není jasné, jak se k samotnému využití této technologie postaví. Nevýhodou je pak bezpečnost celého systému, která má značné nedostatky.

Jak funguje OpenID

OpenID providera nabízí webové rozhraní pro uživatele. V něm uživatel zadá svoje data, která budou přístupná poskytovatelům webových služeb. Od providera získá svoje URL, což je vlastně OpenID.

A Uživatel si na webovém serveru zvolí, že se chce přihlásit pomocí OpenID. **B** Uživatel zadá jen své URL místo jména a hesla, a dostane se ke svému účtu.

