Masarykova univerzita
Fakulta informatiky

závěrečná esej do předmětu
PV 070 Digitální knihovny

Shibboleth - authentication system

http://shibboleth.internet2.edu/

Jan Bařinka

28.11.2005

Popis projektu

Projekt Shibboleth má za úkol vytvořit jednotný systém pro řízení přístupu k webovým zdrojům a službám v situaci, kdy přístup je prováděn z různých institucí s různým systémem řízení bezpečnosti. Systém Shibboleth je navržen tak, aby uživatel mající účet ve své domovské instituci mohl s využitím tohoto účtu přistupovat k webovým zdrojům v jiné instituci. Pro uživatele tak odpadá nutnost znát množství různých přístupových hesel. Správci služeb nemusí řešit problémy s velkým množstvím účtů a s hromadným zřizováním účtů nových, což je dáno především metodou ověřování přístupu na základě atributů.

Průběh projektu

Projekt Shibboleth vznikl pod křídly sdružení Internet2, jehož cílem je vývoj a rozšiřování pokročilých síťových technologií v oblasti výzkumu a výuky na vysokých školách. V současné době Internet2 sdružuje přibližně 200 vysokých škol a spolupracuje s mnoha státními i soukromými organizacemi.

První oficiální dokument o projektu Shibboleth vznikl na konferenci Early Harvest v září roku 1999 v Denveru v USA. V tomto dokumentu jsou stanoveny základní vlastnosti a cíle projektu. Mezi hlavní vytyčené body patří:

- vytvoření modulu pro webový server Apache
- vytvoření kvalitní dokumentace
- zveřejnění sady volně šiřitelných podpůrných programů včetně jejich zdrojových kódů
- vytvoření modulárního a přenositelného softwarového rozhraní pro programování aplikací s podporou systému Shibboleth

V květnu roku 2001 byla vytvořena první verze návrhu specifikace systému. V červnu 2003 vychází první oficiální verze systému.

Mnoho velkých institucí začíná pracovat na nasazení systému Shibboleth v praxi. Za zmínku stojí využití systému Shibboleth v projektu S.F.X. společnosti Ex Libris, která je mimo jiné autorem produktu Aleph užívaného Masarykovou univerzitou. Projekt S.F.X. se zabývá propojením digitálních knihoven. Zájem o Shibboleth projevuje i nakladatelství Elsevir.

V současné době je možné z domovské stránky projektu získat software verze 1.3. Software se skládá ze dvou hlavních částí. Jedna část je napsána kompletně v jazyce Java, a je tak nezávislá na použitém hardwaru a operačním systému. Druhá část je předpřipravena v podobě instalačních balíčků pro systémy Solaris, Fedora Core, Mac OS-X a Microsoft Windows. K dispozici je samozřejmě i balíček zdrojových kódů.

V současnosti užívá sytému Shibboleth mnoho významných institucí i mimo oblast školství. Významná je především důvěra, kterou do projektu Shibboleth vložila organizace Online Computer Library Center. To do jisté míry zaručuje, že projekt a technologie s ním spojené budou prosazovány i v budoucnu.

Cíle projektu

Hlavním cílem projektu je navrhnout a vytvořit systém, který by zjednodušil autentizaci a řízení přístupu k webovým službám v prostředí, které je tvořeno množstvím různorodých institucí. Záměrem tedy je, jednoduše řídit přístup jednotlivců a skupin z různých institucí k webovým službám. Hlavní důraz je kladen na jednoduchost použití a na bezpečnost osobních údajů uživatelů.

Ke splnění cílů musí být užito standardizovaných nástrojů a postupů tak, aby vytvořený systém byl schopný spolupracovat s jinými bezpečnostními systémy.

Pro příklad uveďme následující modelovou situaci. Národní knihovna poskytuje přístup ke svému archivu digitálních dokumentů. Je dohodnuta spolupráce mezi Národní knihovnou a vysokými školami v tom směru, že žáci určitých předmětů mají mít bezplatný přístup k digitálnímu archívu. Představme si konkrétně žáky předmětu PV070 Digitální knihovny na Masarykově univerzitě.

Běžně by se tento problém řešil tak, že by vyučující předmětu zaslal na počátku semestru do Národní knihovny seznam žáků, kteří mají mít po dobu jedné čtvrtiny roku přístup k archivu. Žáci by obdrželi nové přihlašovací údaje.

Užitím systému Shibboleth by se situace zjednodušila následujícím způsobem: Národní knihovna by nastavila řízení přístupu tak, aby k archívu mohl přistupovat uživatel, který je studentem vybrané vysoké školy a který navštěvuje předmět, opravňující ho archivu využít. Pro autentizaci uživatele je užit bezpečnostní mechanismus jeho domovské instituce. V našem případě jde o Informační systém Masarykovy univerzity. Tento bezpečnostní mechanismus vydá prohlášení, že uživatel je studentem a že studuje patřičný předmět. Toto prohlášení je zasláno systému Národní knihovny, a ten na jeho základě umožní či zamítne přístup uživatele k digitálnímu archívu. Správa přístupu je tedy zcela v moci správců domovských institucí. V našem modelovém případě by tato správa mohla být zcela automatizována.

Popis funkce systému

Systém Shibboleth je složen ze dvou základních součástí, které spolupracují. První část systému běží na straně provozovatele poskytované webové služby a jmenuje se Poskytovatel Služeb (SP – Service Provider). Druhá komponentu provozuje domovská instituce uživatele, který se k poskytované službě připojuje. Jmenuje se Poskytovatel Identity (IdP – Identity Provider) Tyto komponenty běží sice nezávisle, ale během provozu spolupracují.

Procedura přihlášení uživatele k webové službě s pomocí systému Shibboleth probíhá následovně:

1. Uživatel pomocí svého webového prohlížeče navštíví požadovanou zabezpečenou webovou stránku. Server, na kterém stránka běží, však vyžaduje údaje o uživateli, aby mohl rozhodnout, zda má uživatel ke stránce přístup.

2. Shibboleth Service Provider, ve snaze zjisti informace o uživateli, provede přesměrování uživatelova prohlížeče na službu zvanou WAYF (where are you from – odkud jsi). Tato služba nabídne uživateli seznam institucí, jejihž uživatelé mohou přistupovat k webové službě.

3. Uživatel za pomoci WAYF služby zvolí svou domovskou instituci. Uživatelův webový prohlížeč je přesměrován na přihlašovací službu uživatelovy domovské instituce. Tato stránka je uživateli známá a uživatel zde provede přihlášení za pomocí jemu dobře známých přihlašovacích údajů. Přihlašovací stránka spolupracuje se službou Shibboleth Identity Provider, která na základě přihlašovacích údajů vydá takzvané prohlášení.

4. Uživatelův prohlížeč je opět přesměrován a to na původně požadovanou webovou stránku. K požadavku je připojena správa obsahující prohlášení od služby Identity Provider. Na základě tohoto prohlášení provede Service Provider prvotní ověření a vyžádá si od Identity Providera soubor atributů, které specifikují uživatele. Na základě těchto atributů se poskytovatel webové stránky rozhodne, zda má uživatel ke službě přístup.

Pokud je již uživatel přihlášen v domovském bezpečnostním systému, pak může být tento krok vynechán. Vynechán může být i krok výběru domovské instituce, například užitím cookie v uživatelově prohlížeči.

Velmi důležitou vlastností procesu ověření uživatele a rozhodnutí o povolení přístupu je takzvané ověřování na základě atributů. Toto znamená, že Identity Provider poskytne jen informace o určitých vlastnostech uživatele. Vlastností uživatele se myslí například jeho příslušnost do skupiny uživatelů nebo to, zda má uživatel zapsán určitý předmět. Tato metoda má dvě zásadní výhody.

Jednou z výhod je, že uživatel sám rozhodne o tom, jaké atributy o něm budou odeslány poskytovateli služby. Tímto je dbáno na zachování soukromí uživatele. Samozřejmě může ale dojít k situaci, kdy poskytovatel služby vyžaduje o uživateli informace, které uživatel poskytnout nechce. Pak záleží na každém jedinci, jak se rozhodne.

Druhou výhodou je absence dodatečného zjišťování informací o uživateli. V současnosti je běžné, že poskytovatel obdrží identifikátor uživatele a sám si o uživateli zjišťuje potřebné informace. Architektura systému Shibboleth je navržena tak, že poskytovatel služby může pracovat jen s těmi atributy, které na základě rozhodnutí uživatele obdrží od Identity Providera.

Veškeré vlastnosti systému a komunikace mezi komponentami systému jsou zapsány ve značkovacím jazyce SAML, který je postaven na XML. Jazyk SAML byl vytvořen ve spolupráci mnoha bezpečnostních expertů jak z oblasti akademické tak průmyslové. Důležitá je především spolupráce komponent systému Shibboleth s cizími přihlašovacími službami. Většina těchto služeb již naštěstí podporuje SAML.

Ke vzniku jazyka SAML a vlastně i ke vzniku projektu Shibboleth přispěl rozvoj federativních identit. Technologie federativních identit umožňuje institucím využít jejich přihlašovacích služeb k prokázání identity u jiných spřátelených institucí. Jde tedy právě o tu oblast internetové komunikace, kterou pokrývá projekt Shibboleth.

Zhodnocení projektu

Systém Shibboleth nebo jeho nástupce má bezesporu budoucnost. Každý uživatel internetové sítě denně přistupuje k mnoha službám, u nichž musí prokazovat svou identitu. Tyto služby můžeme rozdělit do několika skupin. Uvážíme-li například služby, které již poskytuje, či v budoucnu bude poskytovat státní správa, pak se nám objeví jasný příklad jedné takové skupiny, ve které je výhodou užít jednu identitu pro přístup ke službám, které poskytují různé instituce.

Technologie řízení přístupu na základě atributů je z pohledu ochrany osobních údajů jasným krokem vpřed a je jednou z hlavních výhod systému. Dovolil bych si tvrdit, že bez této vlastnosti by systém měl poloviční hodnotu.

Z pohledu Masarykovy univerzity je zajímavé sledovat aktivitu okolo nasazení Shibbolethu v elektronickém výukovém systému Moodle. Pokud je mi známo, v současné době se systémem Moodle experimentuje Filosofická fakulta. Každý uživatel Moodlu musí pro přihlášení zadat své UČO a sekundární heslo, které si zvolil v Informačním systému MU a které se liší od hesla primárního. Tato nejednotnost by mohla být jednou z mnoha věcí, kterou by nasazení systému Shibboleth vyřešilo.

Literatura

Shibboleth Project - Internet2 Middleware, Internet2, 2005
http://shibboleth.internet2.edu/

Michael R. Gettes, Bob Morgan, Keith Hazelton, Paul Hill, Ken Klingenstein, Mark Poepping, Frank Grewe, *Shibboleth Middleware Web Authentication Project*, Internet2, 1999
http://shibboleth.internet2.edu/docs/shibboleth-project.html

R. L. Morgan, Scott Cantor, Steven Carmody, Walter Hoehn, and Ken Klingenstein, *Federated Security: The Shibboleth Approach*, EDUCAUSE Quarterly,Volume 27 Number 4, 2004
http://www.educause.edu/apps/eq/eqm04/eqm0442.asp

SWITCH - AAI – Demo, SWITCH, 2005
http://www.switch.ch/aai/demo/

Metadata Dublin Core

Dublin Core atribut s kvalifikátorem	**Schéma**	**Hodnota**
Title		Shibboleth - authentication system
Title.alternative		závěrečná esej do předmětu PV 070 Digitální knihovny
Creator.personalName		Bařinka, Jan
Creator.address		jan@barinka.net
Subject		Shibboleth
Subject		řízení přístupu
Subject		federativní identita
Description.tableOfContents		Esej na téma Shibboleth - authentication system
Date.created	W3C-DTF	2005-11-28
Type	DCMIType	Text
Format	IMT	application/pdf
Format.medium		computerFile
Format.extent		5 stran A4
Source	URL	http://shibboleth.internet2.edu/
Source	URL	http://shibboleth.internet2.edu/docs/shibboleth-project.html
Source	URL	http://www.educause.edu/apps/eq/eqm04/eqm0442.asp
Source	URL	http://www.switch.ch/aai/demo/
Language	RFC3066	cze