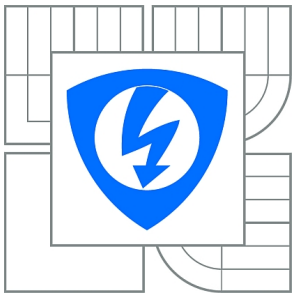
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

SYSTÉMY JEDNOTNÉHO PŘIHLÁŠENÍ

SINGLE SIGN-ON SYSTEMS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

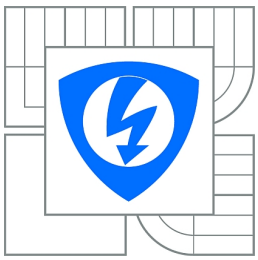
AUTOR PRÁCE — ENDRE TAKÁCS

AUTHOR

VEDOUCÍ PRÁCE — Ing. ONDŘEJ MORSKÝ

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Endre Takács	***ID:***	115293
Ročník:	3	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Systémy jednotného přihlášení

POKYNY PRO VYPRACOVÁNÍ:

Úkolem práce je popsat systémy jednotného přihlášení (SSO) používané v rozlehlých počítačových sítích. Student by se měl zabývat architekturami jako je SecurID, domény systému windows, ale také webovými službami jednotného přihlášení. Praktickou částí práce je návrh webové služby, která umožní přihlášení libovolným již existujícím účtem bez nutnosti registrace.

DOPORUČENÁ LITERATURA:

[1] SURHORE, Lambert, TENNOE, Mariam, HENSSONOW Susan. Windows Server Domain. Betascript Publishing,
2010. 174s. ISBN: 978-6132266194
[2] PROSISE, Jeff. Programování v Microsoft .NET, Webové aplikace v C#, ASP.NET a .NET Framework.
Computer Press, 2003. 736s. ISBN: 80-7226-879-1

Termín zadání:	7.2.2011	***Termín odevzdání:***	2.6.2011

Vedoucí práce: Ing. Ondřej Morský

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Bakalárna práca sa zaoberá s jednotným prihlásením . Opisuje vyskitujúce sa systémy používané v rozsiahlych počítačových sietiach, zabezpečovacie možnosti, integráciu do operačného systému Microsoft Windows. Druhá časť sa zaoberá s webovým rozhraním pre jednotné prihlásenie, kde sú uvedené základné pojmy a princípi fungovania. Zameriava sa na technológiu OAuth, ktorá je využitá pri vytvorení praktickej časti bakalárskej práce.

KLÚČOVÉ SLOVÁ

Jednotné prihlásenie, bezpečnosť, Kerberos, Active Directory, webové rozhranie jednotného prihlásenia, OAuth

ABSTRACT

The subject of this bachelor thesis is the so-called single sign-on technology in context of access control methods. It describes the solutions used in wide computer systems, options of implementing security and integration into the Microsoft Windows operating system. The next part specifies the web interface of this technology, where the explanation of the basic terms and principals are also included. It is focused on the Oauth, which will be used in the practical part of work.

KEYWORDS

Single Sign-On, security, Kerberos, Active Directory, Web Single Sign-On, OAuth

TAKÁCS, E. *Systémy jednotného přihlášení*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2010. 21 s. Bakalářská práca. Vedoucí práce: Ing. Ondřej Morský.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Systémy jednotného přihlášení jsem vypracoval samostatně pod vedením vedoucího semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této semestrální práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu své bakalářské práce Ing. Ondřej Morský za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé semestrální práce.

V Brně dne ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

V dnešnej dobe, ako informačné systémy sa čoraz rýchlejšie rozmnožujú , pre podporu obchodných procesov, pre užívateľov, pre továrenských nástrojov koordinované s počítačmi, pre operačné systémy, pre webové rozhranie ďalej aj pre systémy kde sa nachádza dialóg prístupu medzi užívateľom a administrátorom poskytujúce služby.

Tu užívatelia a správcovia systému zápasia čoraz zložitejším rozhraním splniť svoje pracovné funkcie. Administrátory sa pokúsia čo najlepšie vyhovieť k požiadavkám užívateľov. Tie opatrenia sú najmä orientované na bezpečnosť osobných údajov a v druhom rade,čo najľahšie pracovať v danom systéme.

Pri takýchto systémoch najčastejšie pri začiatku, v iných prípadoch behom práce, užívateľ pristane k bodu, keď sa musí autentizovať, aby mohol pokračovať v práci.V súčasnosti užívatelia pracujú s viacerými informáciami z rôznych systémových zdrojov. A problém začína, keď sa užívatelia zvyčajne majú podpísať na viacerých systémoch, ktoré vyžadajú zodpovedajúci počet prihlásení z ktorých každý môže zahŕnať rôzne užívateľské meno a autentizačné informácie. Vtedy sa správcovia systému stretávajú so správou používateľských účtov čoraz viac.

Správcovia, aby zjednodušili prácu so systémami previedli funkciu jednotné prihlásenie (Single Sign-On, SSO). Je to vlastnoť riadenia prístupu viacerých príbuzných, ale nazávislých softvérových systémov. Vďaka tejto vlastnosti sa používateľ prihlási iba raz a získa prístup ku všetkým systémom, bez toho aby bol vyzvaný k prihláseniu opäť u každého z nich.

1 POPIS PROBLÉMU, ŠPECIFIKÁCIA CIEĽU

Jednou z najväčších problémov komunikácie v počítačových sietiach je otázka zabezbečenia proti zneužitiu ďalšou osobou. Na začiatku vývoja boli siete určené len pre pár vyvolených a preto nebol kladený taký dôraz na ich zabezpečenie. S postupom času, s masívnym rozšírením medzi bežných užívateľov pripojené k internetu, už je zabezpečenie siete stále aktuálnejšou témou. Za najnebezpečnejšie sa všeobecne považuje verejné prostredie internetu, ale chránené pred prípadnými útokmi nie sú chránené ani privátne siete. Tí môžu byť, v prípade pripojenia k internetu, vybavené bezpečnostnou hradbou (Firewallom), ktorá obmedzuje prevoz len na povolené služby, ale netreba vylúčiť útoky z vnútra siete. Je preto vhodné pokladať také prostredie vo vnútri systému za nedôverihodné, a pokúsiť sa ho maximálne zabezpečiť. V tejto práci sa preto zaoberám s oblasťou bezpečnej autentizácie užívateľov pre prostredie v privátnych sieťoch. V dnešnej dobe sú už rôzne existujúce riešenia. Sem patrí aj jednotné prihlásenie (Single Sign-On, SSO). V ďalších krokoch prevediem opis o systémoch používaných v dnešných sietiach, architektúry možných zabezpečení. V druhom časti sa zaoberám stručnejším opísaním Web Single Sign – On.

2 ROZBOR SINGLE SIGN-ON

2.1 Úvod do Single Sign – On

Prihlásenie je ťažké urobiť, najmä ak si musíme zapamätať rôzne užívateľské mená a heslá pre každý jednotlivý systém alebo zdroj. Ak používáme heslá, ktoré sú ľahko zapamätateľné, alebo jedno heslo pre všetky svoje účty, bezpečnostných špecialistov rýchlych prstov: "ľahko zapamätateľné" tiež znamená "ľahko uhádnuteľné." Odborníci varujú pred opakovaním hesiel alebo písanie hesiel niekam na papier, že by to útočník mohol nájsť. A dodávajú, že by sme mali zmeniť často každé heslo.

IT manažéri príjmajú myšlienku Single Sign-On (SSO), ktorá v posledných rokoch môže výrazne a administratívne znížiť služby ba aj podporné náklady. Celkové životné prostredie môže byť bezpečnejšie, používatelia môžu len jedno heslo zabudnúť.

Single Sign On, je proces autentifikácie, ktorý umožňuje užívateľovi zadať užívateľské meno a heslo iba raz pri prihlásení na server, ale majú prístup k mnohým aplikáciám. Ak má používateľ právo na používanie rôznych aplikácií na serveri, má sa prihlásiť len raz a nebude vyzvaní znova zadať užívateľské meno a heslo zakaždým, keď chce prepnúť na iný program alebo aplikáciu v homogénnom systému.[1]

2.2 Výhody Single Sign – On

- Zníženie prevádzkových nákladov
- Znížený čas na prístup k dátam
- Vylepšené užívateľské skúsenosti
- Pokročilé bezpečnostné systémy
- Silná autentizácia
- Jednoduché zaťaženie vývojárov
- Centralizované správy používateľov a rolí

2.3 Typi Single Sign – On

2.3.1 Integrovaný Single Sign-On do operačného systému

Tieto služby nám umožnia pripojiť sa k viacerím aplikáciám v rámci našej siete, ktoré používajú spoločné autentizačné mechanizmy. Tieto služby overujú žiadosti poverovacích lístkov po prihlásení do siete, a podľa toho používajú poverenia určiť akcie, ktoré môžeme vykonávať na základe užívateľských práv. Napríklad, ak aplikácia je integrovaná pomocou Kerberos, systém overí mandáty užívateľa, a môžeme pristupovať k ľubovoľným zdrojom v sieti, ktorá je integrovaná s Kerberos. [2]

2.3.2 Extranet Single Sign-On

Tieto služby nám umožnia prístup k prostriedkám cez Internet pomocou jediného súboru poverenia používateľa. Užívateľ poskytuje sadu poverenia pre prihlásenie k rôznym webovým stránkam, ktoré patria k rôznym organizáciám. Príkladom tohto typu Single Sign-On je Microsoft Passport Network pre spotrebiteľa-aplikácie. Pre federalizované scenáre, Active Directory Federation Services umožňuje Web SSO. [2]

2.3.3 Server-based Intranet Single Sign-On

Tieto služby umožňujú prepojiť viac heterogénnych aplikácií a systémov v podnikovom prostredí. Tieto aplikácie a systémy nemusia používať spoločné overenia. Každá aplikácia má svoj vlastný užívateľský adresár úložiska. Napríklad, v organizácií, systém Windows používa adresárovú službu Active Directory pre autentifikáciu používateľov, sálové počítače IBM používajú Resource Access Control Facility (RACF) na overenie rovnakých účtov. V rámci podniku sú aplikácie a integrácie front-end a back-end aplikácií. [2]

Okrem toho, synchronizácia hesiel zjednodušuje správu databázy SSO, a drží heslá synchronizované cez užívateľské adresáre. Je možnosť urobiť pomocou adaptérov synchronizácie hesiel, ktoré je možno konfigurovať a spravovať pomocou nástrojov synchronizáciu hesiel. [2]

2.3.4 Enterprise Single Sign-On

Enterprise Single Sign-On poskytuje služby pre ukladanie a prenos šifrovaných poverení používateľa v rámci lokálnej siete a hraníc domény. SSO skladuje poverovacie listiny v databáze prihlasovacích údajov. Pretože SSO poskytuje univerzálne single sign-on riešenie,tak môže middleware aplikácie a vlastné adaptéry využiť, bezpečne ukladať a prenášať užívateľské poverenia v rámci životného prostredia. Koncoví užívatelia nemusia pamätať rôzne poverenia pre rôzne aplikácie. [2]

2.4 Bezpečnosť u Single Sign – On

Pôvodným cieľom jednotného prihlásenia bolo zníženie počtu hesiel a teraz sú použité aj iné formy autentifikácie používateľov, ako sú certifikáty PKI, čipové karty, tokeny a biometrické prvky, môžu byť tiež súčasťou súčasnej SSO riešenia. ID užívateľa, ale nie je primárnou funkciou riešenia SSO. V skutku sa spoliehajú na úplne samostatné autentizačné mechanizmy.

2.4.1 PKI certifikáty

Public Key Infrastructure (PKI) je súbor hardvéru, softvéru, ľudí, politiky a postupy potrebné pre vytváranie správ, distribúcií, používaní, skladovaní, a zrušenie digitálnych certifikátov. V kryptografii , PKI je usporiadanie, ktoré sa viaže k verejnej kľúči s príslušnými užívateľskými identitami pomocou certifikačnej autority (CA). Identita užívateľa musí byť unikátne v rámci každej domény CA. Väzba je stanovená prostredníctvom registrácie a vydávania procesov, ktoré v závislosti na úrovni zabezpečení viažu, môžu byť vykonané pomocou softvéru na CA, alebo pod dohľadom človeka. Úloha PKI, ktorá zaisťuje túto väzbu sa nazýva Registračná autorita (RA). Pre každého užívateľa, identitu užívateľa, verejný kľúč, ich väzbu, podmienky platnosti a ďalšie atribúty sú vyrobené v nezabudnuteľnom certifikáte verejného kľúča vydané pomocou CA. [6]

U SSO sa používa certifikácia X.509. V kryptografii , X.509 je ITU-T štandard pre infraštruktúru verejných kľúčov (PKI) pre Single Sign-On (SSO) a Privilege Management Infrastructure (PMI). X.509 špecifikuje, okrem iného, štandardné formáty pre certifikáty verejného kľúča , zoznamy odvolania osvedčenia , certifikáty atribút , a certifikačné cesty overenia algoritmu. [6]

2.4.2 Čipové Karty

Čipové karty môžu poskytovať identifikáciu, autentifikáciu, ukladanie dát a spracovanie žiadostí.

Výhody čipovej karty priamo súvisia s množstvom informácií a aplikácií, ktoré sú naprogramované pre použitie na karte. Jednotné kontaktné miesta môžu byť programovateľné pre verejný dopravný nárok, vernostné programy a klubové členstvo, aby som vymenoval len niekoľko.Bezkontaktná čipová karta môže byť naprogramovaná s viacerými bankovými poverovacími listinami , na lekárske nároky a ako vodičský preukaz. Multi-faktor a blízkosť autentizácie môže byť vložený do čipovej karty na zvýšenie bezpečnosti všetkých služieb na karte.Napríklad môže byť čipová karta naprogramovaná povoliť len pre bezkontaktné transakcie, pokiaľ to je tiež v dosahu iného zariadenia, ako jednoznačne spárovaný mobilný telefón. To môže výrazne zvýšiť bezpečnosť.

2.4.3 Tokeny

Môžu byť označované ako raz použiteľné one-time password tokeny, dvoj-faktorové autentizácie.

One-Time Password (OTP) je heslo, ktoré je platné len pre jeden login úlohu alebo transakciu. Jednorázové heslá môžu zabrániť, aby pri krádeži útočník vedel využiť heslá lebo pri dlhšom čase heslá budú neplatné. Najdôležitejší problém jednorázových hesiel je, že nemôžeme ich viackrát používať.

Pod dvoj-faktorovou autentizáciou (TFA - Two- Factor Authentication) sa

rozumie použitie akýchkoľvek nezávislých autentizačných metód (napr. heslo, hodnota z fyzického tokena) pre zvýšenie istoty, že nositeľ bol povolený na prístup k bezpečnému systému. Zvyčajne užívateľské meno je známe, a ozýva sa po prístupe, preto nie sú chápané ako bezpečnostné informácie. Táto spätná väzba však zaisťuje správnu voľbu účtu akcie používateľa.

2.5 Služby

Čiastkové služby Single Sign-On (SSO):

- Mapovanie: Mapovanie užívateľských účtov v systémoch
- Vyhľadávanie: Vyhľadá poverenia užívateľa v databáze poverenia v back-end systémov. Jedná sa o dynamické komponenty SSO.
- Správy: Spravujú v pridružených aplikáciach a mapujú v každých prijatých prihláškach.
- Tajomstvo: Generuje tajne a distribuuje ju do ostatných serverov v systéme. To je aktívne len na Single Sign-On servery, ktoré funguje ako Master Secret Server.
- Synchronizácia hesiel: Zjednodušuje správu databázy poverenia SSO, a drží heslá synchronizované cez užívateľské adresáre

2.6 Server

Server môže vykonávať niektoré z týchto úloh:

• Funguje ako Master Secret Server. Master Secret Server drží hlavné tajomstvo, alebo šifrovací kľúč, ktorý sa používa na zašifrovanie všetkých mandátov v systéme SSO. Hoci Master Secret Server môže fungovať ako server pre vyhľadávanie a správu,

• Vykonáva administratívne činnosti. SSO administrátori môžu využiť niektoré z Single Sign-On servery vykonávať administratívne úlohy, ako je riadenie pridružených aplikácií, nastavenia poverenia užívateľa a správu užívateľských zobrazení.

• Zvláda vyhľadávanie operácií. SSO server používa runtime komponenty pozrieť do poverenia používateľa.

• Pri problémoch zachraňuje vstupenky servera SSO a tiež zachraňuje SSO lístky, ktoré aplikácie môžu použiť na získanie poverenia používateľa.

• Synchronizácia hesiel. Užívateľ si môže vytvoriť a spravovať synchronizácie adaptérov hesiel na serveri SSO.

3 SINGLE SIGN-ON VO WINDOWSU

Microsoft Windows operačný systém poskytuje integrované, komplexné a ľahkopoužiteľné SSO schopnosti. SSO je poskytovaná natívne v systéme pomocou vstavanej Kerberos a Secure Sockets Layer protokolov, ktoré tiež môžu poskytovať štandardy SSO v zmiešaných sietiach. Microsoft SNA Server ďalej rozširuje tieto možnosti na mainframe prostredí prostredníctvom ich preplietarne protokoly. Homogénne siete založené na Windows teraz sú ľahko zvládnuteľné, majú bezproblémové SSO schopnosti, ale pretože jeho široké interoperability(schopnosť systémov vzájomne si poskytovať služby a efektívne spoluprocavať), Windows môže byť dobrou voľbou ako sprostredkovateľ SSO medzi rôznorodnými systémami v heterogénnej sieti.

3.1 Výhody

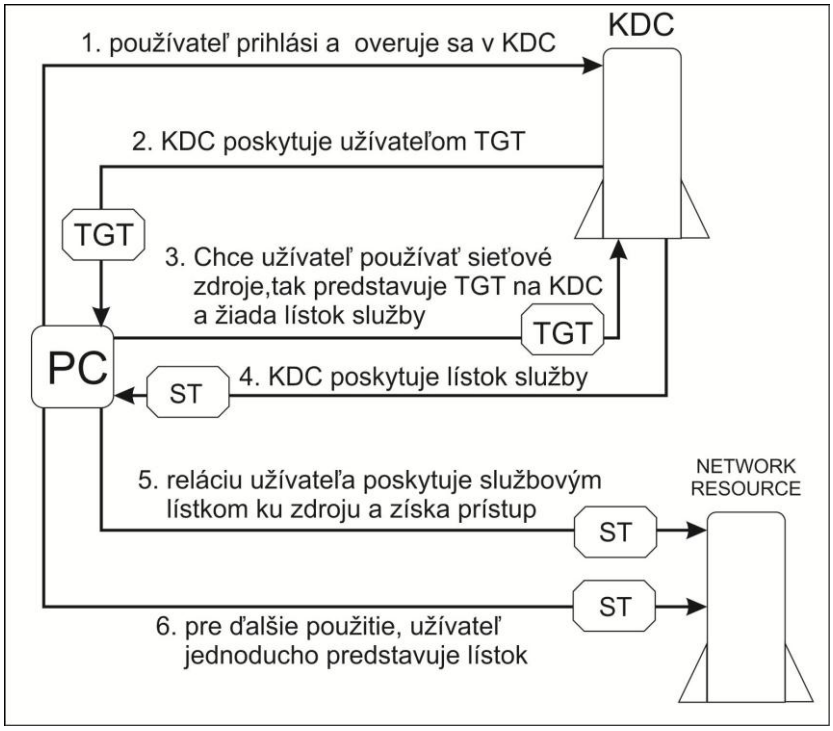
- Jednoduchšia správa. Primárnou prekážkou prijatia pre väčšinu implementácií SSO je, že sú priskrutkované na operačný systém a pridané do správce záťaže, ktoré ho vyžadujú alebo ho vykonajú SSO špecifické úlohy,s pomocou SSO-špecifických nástrojov. Pod Windows SSO-súvisiace úlohy sú vykonávané transparentne v rámci bežnej údržby, použitia rovnakých nástrojov, ktoré sú použité pre iné administratívne úlohy.
- Všetky siete, správa informácií v systéme Windows, vrátane všetky SSO špecifické informácie sú uložené v jednom úložisku, Active Directory adresárovej služby. To znamená, že tam je jediný autoritatívny zoznam každého užívateľa ,správy a výsady. To umožňuje správcovi zmeniť oprávnenia užívateľa a vedia, že výsledky budú propagovať cez širokú sieť.
- Lepšie zabezpečenie siete. Používatelia po viacerých prihlásení sú už zapadnutí, a preto nie je nutné pamätať si viac hesiel pre prístup k sieťovým zdrojom. To je tiež prínosom pre help desk pracovníkom, ktorí potrebujú o polovicu menej žiadostí o zabudnuté heslá.
- Všetky dostupné SSO metódy pod Windows poskytujú bezpečnú autentifikáciu a poskytujú základ pre šifrovanie relácie užívateľa v sieťovom prostriedku. Nakoniec, pretože konsolidáciou informácií pre správu v siete v rámci služby Active Directory môže správca s istotou vedieť, že keď sa zakáže užívateľský účet, je účet plne invalidný.

3.2 Kerberos

SSO je poskytovaná natívne vo Windows domén pomocou protokolu overovania Kerberos, čo je predvolený protokol pre overovanie používaných systémov.Použitie protokolu Kerberos poskytuje významné zlepšenie jednoduchosti v správe, v bezpečnosti a výkonu siete.

Protokol Kerberos je založený na myšlienke vstupeniek, zašifrované dáta pakety vydané dôverihodnou autoritou tzv Key Distribution Center (KDC). Vstupenka ručí za identitu užívateľa, rovnako ako účtovník ďalších informácií. KDC zaisťuje vstupenky pre všetkých používateľov v rámci jeho miestneho orgánu, alebo oblasti. V systéme, každý radič domény je KDC, a oblasť radiče domény zodpovedá jeho domény. [5]

Prevádzka protokololu je jednoduchá, ako je znázornené na Obrázok 3.1. V čase prihlasovania, používateľ autentifikuje na KDC, ktorá jej poskytuje počiatočný lístok Ticket Granting Ticket (TGT). TGT je malý, zašifrovaný súbor pre identifikáciu s obmedzenou dobou platnosti. Keď používateľ potrebuje využívať sieťové zdroje, jeho užívateľské relácie predstavuje TGT na radič domény a požiada o lístok pre konkrétny zdroj, tzv lístok služby (ST – Service Ticket). On predstavuje ST na zdroj, ktorý mu poskytuje prístup. [3]



Obrázok 3.1: Prevádzka protokolu Kerberos

Integrácia protokolu Kerberos v systéme Windows poskytuje administratívny a bezpečnostný jednoduchý model, efektívne riadenie a kontrolu užívateľov a sieťových

prostriedkov. Softvér Kerberos funguje na vrchole operačného systému v normálnej bezpečnostnej architektúry, nie ako jej časť, vyžadujúce SSO-konkrétne informácie majú byť skladované,oddelené od ostatných systémových informácií a núti správcu učiť sa ďalšie administratívne nástroje výhradne za účelom riadenia infraštruktúry SSO. [3]

Avšak, je protokol Kerberos plne integrovaný do systému Windows, Kerberos je neoddeliteľnou súčasťou systému bezpečnostnej architektúry, naozaj to je predvolená metóda overovania. SSO-súvisiace informácie sú uložené v adresári Active Directory spolu so všetkými ďalšími informáciami o sieťové objekty.[3]

3.3 Active Directory

Active Directory je štruktúra hierarchických rámcových objektov . Objekty možno rozdeliť do dvoch širokých kategórií: zdroje (napr. tlačiarne) a objekty zabezpečenia (užívateľa alebo počítača účty a skupiny). Zabezpečenia sú objekty služby Active Directory, ktoré sú priradené unikátne identifikátory zabezpečenia (SID) používané na kontrolu prístupu a nastavenie zabezpečenia. [4]

Každý objekt predstavuje jeden subjekt - či používateľ, počítač, tlačiareň, alebo skupina - a jeho atribútov. Niektoré objekty môžu byť aj kontajnery iných objektov. Objekt je jednoznačne identifikovaná svojím menom a má sadu atribútov - vlastností a informácie, ktoré objekt môže obsahovať - definované schéma, ktoré tiež určujú typy objektov, ktoré môžu byť uložené v službe Active Directory.

Každý atribút objektu môže byť použitý v niekoľkých rôznych objektov schémy triedy. Každý objekt schémy je neoddeliteľnou súčasťou definície objektov služby Active Directory, deaktivácia alebo zmena týchto objektov môže mať vážne následky, pretože sa bude zásadne meniť štruktúru Active Directory sám.

Všetky objekty vo vnútri spoločného adresára, databázy, sú známe ako domény. Každá doména obsahuje informácie iba o objektoch, ktoré patria do tejto domény. Strom sa skladá z jednej domény, alebo viac domén v súvislom mennom priestore. Les je zbierka stromov a predstavuje najvzdialenejšie hranice, v ktorom existujú užívatelia, skupiny počítačov, a iné objekty. Les je bezpečnostná hranica pre službu Active Directory.

Active Directory rámec, ktorý drží objekty si môžme prezrieť na niekoľkých úrovniach. Na vrchole štruktúry je les. Les je zbierka viac stromov, ktoré zdieľajú spoločný globálny katalóg, adresár schémy, logická štruktúra a konfigurácie adresára. Les, strom, doména sú logických častí v sieti služby Active Directory.

Active Directory lesu obsahuje jeden alebo viac tranzitívne dôvery spojených stromov. Strom je kolekcia jedného alebo viacerých domén a doménové stromy v súvislých menných priestoroch, opäť súvisia s tranzitívnou dôveryhodnosťou hierarchie. Domény sú identifikované podľa ich štruktúrového mena a mena priestoru .

3.4 Jednoduchá správa

Administratívne úlohy možné ľahko vykonať pomocou Microsoft Management Console (MMC), ktorá stanovuje spoločný rámec pre všetky nástroje pre správu. Každý nástroj je balený ako modul a MMC poskytuje spoločné užívateľské skúsenosti a použitie paradigmy. Všetky SSO administratívne funkcie sú implementované pomocou modulu MMC ako Active Directory Manager. [3]

4 WEB SINGLE SIGN-ON

Každý jednotlivec žijúcí v modernej spoločnosti je identifikovateľný veľkým množstvom atribútumov, akým môžu byť napríklad rodné číslo, číslo občianského preukazu, cestovného pasu, vodičského preukazu, číslo kreditnej karty, bankovnému účtu a mnohými dalšími. Elektronickú identitu jednotlivca môžeme však chápať vo väčšom množstve. V horeuvedenom je možné pridať e-mailové adresy, ména a heslá k aplikáciám a systémom, diáre plánovaných schôdzkov, zoznam kontaktov, charakteristické profily záujmov, ale aj elektronicky objednané obedy. Pridáme ktomu výučty spojené najčastejšie s výkonom zamestnania ďalšie uživatelové "odtlačky" pri putovaní internetom (účty verejných poskytovateľov elektronickej pošty, účty v rámci elektronických obchodov, registrácie pri stiahnutí demoverzií softwarových produktov, identitu v diskuzných fóroch, ...), dostaneme pomerne pekný džungel plný menom, heslom a rôznych kódov.

Táto doba, keď každá nová aplikácia si so sebou prinášala vlastný spôsob overenia uživateľov a riadenie prístupových práv, sa pomali stáva minulosťou. Stále viac sa darí presvedčovať dodavateľov nových systémov, aby využívali k overeniu uživateľov autentizačné prostriedky vo firmách. V rámci spoločnosti sa teraz smeruje k tomu, aby uživateľ bol v rámci organizácie identifikovaný v systéme, keď možno len jediným účtom (menom/heslom, osobným certifikátom, atd.).

4.1 Základný popis použitých komponentov

Pre rýchlu orientáciu v texte najprv vymenujem a krátko popíšem komponenty použité v texte.

4.1.1 LDAP

Lightweight Directory Access Protocol je protokol pre poskytovanie adresárových dát. Vychádza z protokolu X.500 a používa sa na uloženie dát podľa RFC2307. Adresárová štruktúra je definovaná schematicky. LDAP sa využíva ako primárna technológia pre publikáciu niektorých informácií v PKI prostrediu, ako napríklad poskytovanie vydaných certifikátov a zoznamov ich revokácie. Používa sa aj pri potrebách správy uživateľov a rovnako ich autentizáciou. LDAP sa používa ako interný mechanizmus celou radou komerčných riešení napr. Active Directory od spločnosti Microsoft alebo riešenie Jednotného prihlásenia pre Oracle Application server od Oracle. [9]

4.1.2 KERBEROS

Ako už bolo napísané protokol je založený na symetrickú kryptografiu (používa stejný klúč pre enkryptovaniu a dekrytpovaniu textu). Na strane klienta sa text zašifruje s pomocou klúča a šifrovacieho algoritmu. Tak vznikne šifrovací text, ktorý sa prenáša cez nezabezpečenú sieť. Na strane serveru sa text s použitím tým istým klúčom a algoritmom sa rozšifruje na pôvodný text. Využíva princíp dôverihodnej tretej strany. [5]

4.1.3 Apache HTTP Server

Apache HTTP Server je softwarový webový server s Open source licenciou pre Linux, BSD, Microsoft Windows a iné platformy. V dnešnej dobe je najrozšírenejším na celom svete. Vývoj Apache začal v roku 1993 v NCSA (National Center for Supercomputing Aplications) na Illinoiskej univerzite. Od apríla 1996 bol Apache najpopulárnejší server na internete. V máji 1999 bežal na 57 % zo všetkých serverov a v apríli 2008 jeho používanosť dosiahla 50,42 % (výsledky merania Netcraft). [10]

4.1.4 KDC

Key Distribution Center je centrum výdaja krb ticketov.V kryptografii KDC je súčasťou kryptografického systému kde má cieľ znížiť riziká spojené s výmenou kľúča . [5]

4.1.5 WWW

World Wide Web je distribuovaný hypertextový internetový informačný systém, v ktorom dokumenty obsahujú odkazy na iné miestne alebo vzdialené dokumenty.Je to oficiálne (nesprávne laické pomenovanie len pre internet) označenie tej časti, kde sa informácie nachádzajú vo forme webových stránok. Každý dokument má svoju špecifickú adresu - URL a je pomocou nej nájdený a zobrazený v programoch nazývaných webový prehliadač. Dokumenty nazývané webové stránky môžu obsahovať hypertextové odkazy. Vďaka týmto odkazom, sú dokumenty navzájom poprepájané a vytvárajú sieť. [7]

4.1.6 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) je zabezpečená verzia HTTP, komunikačného protokolu WWW. Namiesto používania jednoduchej textovej komunikácie, HTTPS šifruje prenos dát použitím SSL (Secure Socket Layer) protokolu alebo TLS (Transport Layer Security) protokolu a tým zaisťuje primeranú ochranu pred odpočúvaním komunikácie a pred útokom. Pre HTTPS komunikáciu sa štandardne

používa TCP/IP port 443. [11]

4.1.7 AES

Advanced Encryption Standard je v kryptografii označené ako symetrické šifrovanie. Pôvodné meno bol Rijndael. Šifrovanie využíva symetrický klúč, tzv. ten istý klúč je použité pre šifrovanie a dešifrovanie. Dĺžka klúča môže byť 128, 192 alebo 256 bitov. Metóda šifruje dáta postupne v blokoch s pevnou dĺžkou 128 bitov. Šifrovanie sa vyznačuje vysokou rýchlosťou šifrovania. V súčastnej dobe nie je známi žiadny prípad plného prelomenia tejto metódy. [8]

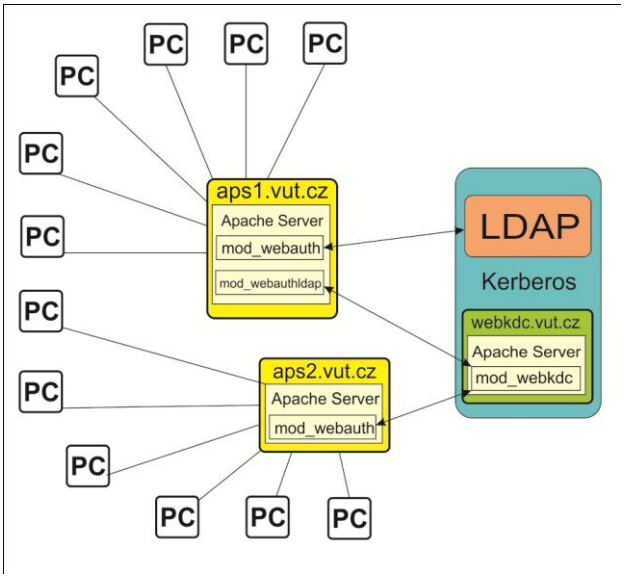
4.2 Single Sign – On riešenie pre Web

SSO riešenie pre web je založené na autentizačnom systéme Kerberos. Celý systém Webovej Autentizácie (WebAuth) je tvorený tromi spolupracujícími modulmi do WWW serveru Apache:

- mod_webauth
- mod_webauthldap
- mod_webkdc.

Srdcom celého systému je login-server bežne nazývaný WebKDC (KDC je prevzatý z názvoslovia systému Kerberos, kde KDC je skratka pre Key Distribution Center). Na WebKDC beží mod_webkdc. Jej úlohou je prijať požiadavky od aplikačných serverov, spracovávať ich a overovať identitu pristupujúceho uživateľa i autentizačnej autorite.

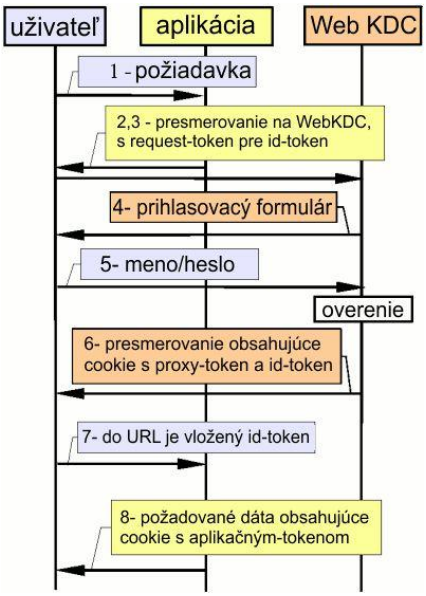
Zostávajúce dva moduly mod_webauth a mod_webauthldap sú umiestnené na aplikačnom servery, na WWW servery Apache, ktorý poskytuje stránky chránené systémom WebAuth. Prvé z modulov zaisťuje overenie doteraz neznámého uživateľa presmerovním na WebKDC server a prijme identitu uživateľa s ním zaslaným cookie, do ktorého si aplikační server skorej túto identitu už overovaného užívateľa uložil. Je vtedy možné povedať, že sa stará resp. vyžaduje autentizáciu uživateľa. Druhý modul, mod_webauthldap, urobí autorizačnú službu. Pomocou sním je možné definovať zoznam povolených skupín uživateľov, ktoré sú spravované s adresárovou službou LDAP. Modul mod_webauth musí byť na aplikačnom serveru vždy. Pomocou sním je možné v konfiguračnom súbore WWW servery Apache povoliť všetkých overených uživateľov alebo ich menovitý zoznam. Modul mod_webauthldap je pre aplikačný server voliteľný. Prostredie založené na webovom SSO riešení WebAuth môže vypadať napríklad tak, ako je znázornený na Obrázok 4.1. [12]



Obrázok 4.1: Schéma k Single Sign – On

4.3 Prvé prihlásenie užívateľa k Single Sign – On

Spracovanie prístupu doteraz neovereného užívateľa v SSO systéme sa zúčastní užívateľ (resp. jeho WWW prehliadač), aplikačný server (webová aplikácia), login-server (WebKDC) a autentizačná autorita (napr. Kerberos). Je nutné pripomenúť, že pre správnu funkciu je vyžadované kryptované (HTTPS) spojenie ako medzi užívateľom a aplikačnom servery, tak i medzi užívateľom a login-serverom. Časová súslednosť jednotlivých akcií nutných pre úspešné overenie užívateľa do webovej aplikácie je vidieť z Obrázok 4.2 .



Obrázok 4.2: Prvé prihlásenie užívateľa k Single Sign – On

1. Neoverený uživateľ pristupuje k webovej aplikácii chráneným WebAuthem.
2. mod_webauth detekuje, že uživateľ doteraz nevlastní aplikačný token (nedostala od nej aplikačný cookie) a vytvorí tzv. request-token pre id-token. Request-token obsahuje informácie ako sú návratové (resp. pôvodne vypočúvané) URL, požadovaný typ tokenu, atď. Request-token je zakryptované s pomocou AES session-klúčom zdielané medzi aplikačným serverom a WebKDC (login-server) získané z webkdc-service-tokenu. mod_webauth tak vytvorí redirekt na WebKDC, ktorý obsahuje request-token v parametrech URL.
3. Redirekt spôsobí presmerovanie prehliadača užívateľa na WebKDC spolu s vygenerovaným request-tokenom. Žiadné cookie nie je poslané na WebKDC (kým žiadny uživateľ nemá).
4. WebKDC potom rozkryptuje request-token. Skontroluje čas vytvorenia, za účelom overenia, že je dostatočne "čerstvý" a pošle späť uživateľskému prehliadaču prihlasovací formulár. Request-token je uložený v skrytej položke tohoto formulára.
5. Uživateľ zadá svoje prihlasovacie meno a heslo a odosiela dáta vo formuláre späť k zpracovaniu na WebKDC.
6. WebKDC overuje zadané meno a heslo a tak skutočnosť, že aplikačný server, ktorý požaduje overenie uživateľa má povolenie vyžadovať id-token. Predpokladejme, že prihlasovacie meno a heslo sú správne, tak WebKDC vytvorí cookie, do ktorého uloží proxy-token a id-token (obsah cookie je kryptované privátnou AES-kľúčom WebKDC). Stránka s potvrdzovaním, že overenie prebehlo v poriadku, je následne poslané do uživateľského prehliadača obsahujúci odkaz na pôvodnú požadovanú stránku.
7. Uživateľský prehliadač znovu pristúpi na pôvodnú požadovanú stránku a v URL parametroch je odovzdaný i id-token (identita) uživateľa.
8. mod_webauth si z požiadavky prevezme id-token a následne skontroluje, že je "čerstvý". Keď je všetko v poriadku, tak prepíše id-token na aplikačný-token a uloží ju do cookie pre ďalšie použitie. Nakoniec je token odstránený z URL (keď nie je potreba - aplikácia verí predloženému cookie, ktorá je kryptovaná s jej privátnym AES klúčom). [12]

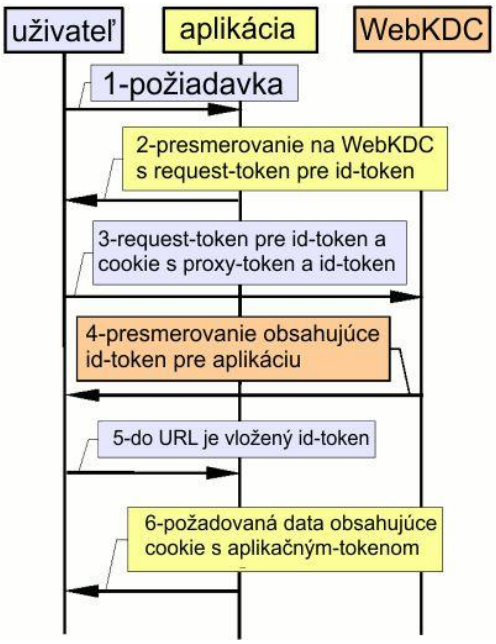
4.4 Užívateľ už je overený v systéme

Keď je uživateľ už úspešne overený pomocou WebKDC, tak prístup ku každej ďalšej aplikácie prebiehá zjednodušeným spôsobom - Obrázok 4.3.

1. Uživateľ pristupuje k webovej aplikácie chráneným WebAuthem.
2. mod_webauth detekuje, že uživateľ doteraz nevlastní aplikačný token (nedostala od nej aplikačný cookie) a vytvorí tzv. request-token pre id-token. Request-token obsahuje informácie ako sú návratové (resp. pôvodne dotazované) URL, požadovaný typ tokenu, atď. Request-token je zakryptovaný použitou AES session-klúčom zdielaným medzi aplikačným serverom a WebKDC (login-server) získaným z webkdc-service-tokenu. mod_webauth tak vytvorí presmerovanie na WebKDC (obsahujúce request-token v parametroch URL).
3. Redirekt spôsobí presmerovanie prehliadača užívateľa na WebKDC spolu s

vygenerovaným request-tokenom. Zároveň je na WebKDC server poslané cookie obsahujúce proxy-token a id-token, ktoré WebKDC server uživateľa už vystavil pri jeho prvotnom overeniu.

4. WebKDC server detekuje z poslaného cookie, že uživateľ má platný proxy-token a používa ju pre vytvorenie nového id-tokenu pre aplikační server. WebKDC následne vygeneruje návratové URL, ktorá obsahuje response-token pre aplikačný server.
5. Uživateľský prehliadač znovu požiadá o pôvodne zadané chránenú stránku a v URL parametre predá aplikačnému serveru id_token už skorej prihláseného uživateľa.
9. mod_webauth si z požiadavky prevezme id-token a následne skontroluje, že je "čerstvý". Keď je všetko v poriadku, tak prepíše id-token na aplikační-token a uloží ju do cookie pre dalšie použitie. Nakonec je token odstranený z URL (keď nie je potreba - aplikácia verí predloženému cookie, ktorá je kryptovaná s jej privátnou AES klúčom). [12]



Obrázok 4.3: Užívateľ už je overený v systéme

5 RIEŠENIE VLASTNEJ SLUŽBY SINGLE SIGN – ON

Praktická časť bakalárskej práce je venovaná k vytvoreniu vlastnej služby Single Sign – On. Aby webová stránka so službou bola najefektívnejšia je potreba dodržiavať určité body technologického postupu. Ktorí sú nasledujúce:

- Vymedzenie problému, cieľ praktickej časti
- Návrh funkcií, ktoré by mala webová stránka obsahovať
- Vybrať správne technológie pre tvorbu portálu
- Vývoj aplikácií, programovanie
- Skontrolovanie správnosti a funkčnosti webovej stránky

5.1 Vymedzenie problému, cieľ praktickej časti

5.1.1 Vymedzenie problému

V dnešnej dobe sa vývojári začali silne zaoberať s pojmom Single Sign – On a vkladajú veľký dôraz pre vývoj tejto služby. Ako mladý vývojár a pozorovateľ nových vlastností v téme konštruovanie webových stránok, ma začal zaujať aj sekcia súvisiace s jednotným prihlásením. Preto som sa rozhodol uchopiť túto príležitosť, formou implementácie už existujúce služby, ktorá dáva príležitosť pre vývoj vlastnej znalosti.

5.1.2 Cieľ praktickej časti

Cieľom praktickej časti mojej bakalárskej práce je návrh internetového portálu so službou Single Sign – On, pričom samotný návrh riešenia sa dá rozdeliť do nasledujúcich bodov:

- Návrh jednoduchého fórumu, ktorá bude ľahko ovládateľná a prispôsobiteľná pre prezentáciu jednotného prihlásenia.
- Implementácia služby jednotného prihlásenia z jedných veľkých poskytovateľov tejto služby. Správne riešenie bude skontrolované pomocou prístupu na portál bez nutnosti registrácie a s pomocou pridaním príspevkom do fórumu.

5.2 Návrh funkcií portálu

Použiteľnosť webu sa zaoberá tým ako intuitívne a ľahko sa užívateľovi web používa, ako je prehľadný a zrozumiteľný. Zjednodušene by sa dalo povedať, že použiteľný web je taký, pri ktorom užívateľ nemusí premýšľať. Cieľom zvýšenia použiteľnosti webu je najmä to, aby uživateľ dokázal splniť svoj cieľ bez toho, aby pri tom robil zbytočné chyby. Použiteľnú webovú stránku dokáže akýkoľvek užívateľ

rýchlo ovládať a efektívne s ním pracovať.

Medzi funkciami portálu bude patriť možnosť pridanie príspevku do fóra po správnom prihlásení. Webový portál bude fungovať k diskusii lubovoľných témam, ktoré budú určovať uživaťelia.Aby užívaťel, ktorý sa len chce pridať príspevok len raz, alebo nechce sa zaregistrovať do fórumu môže využiť funkciu jednotného prihlásenia ktorá bude riešená pomocou Facebook portálu.

5.3 Technológie pre tvorbu portálu a pomocné nástroje

5.3.1 PHP

PHP je voľne šíriteľný populárny open - source skriptovací programovací jazyk, ktorý umožňuje procedurálne, alebo objektovo orientované programovanie. Je predovšetkým vhodný na programovanie klient-server aplikácii na strane servera. Má využitie najmä pre programovanie interaktívnych dynamických www stránok a aplikácií. [10]

Jednoducho sa dá povedať, že skript napísaný v PHP je uložený na strane servera a klient, ktorý ho volá, dostane ako odpoveď klasickú statickú (X)HTML stránku. To znamená, že skript spracuje požiadavku klienta na serveri, na rozdiel napríklad od JavaScript-u, ktorý sa spracuje na strane klienta. Toto riešenie má v porovnaní s PHP výhodu v tom, že nemusíte stránku opätovne načítavať, ale hlavnou nevýhodou takýchto riešení je v možnostiach použitia a hlavne v (ne)bezpečnosti. Keďže útočník vie pozmeniť skript na strane klienta aby vykonal nebezpečný kód, čo je v prípade PHP značne náročnejšie – útočník by sa musel dostať na server. [10]

PHP dokáže spolupracovať s relačnými databázami, ako napríklad MySQL, Oracle, IBM DB2, Microsoft SQL Server, PostgreSQL a SQLite, pričom si stále zachováva jednoduchú a priamočiaru syntax. [10]

5.3.2 MySQL

MySQL je slobodný a otvorený viacvláknový, viacužívateľský SQL relačný databázový server. MySQL je populárny databázový systém, podporuje viacero platforiem ako Linux, Windows či Solaris a je implementovaný vo viacerých programovacích jazykoch ako PHP, C++ či Perl. Databázový systém je relačný typu DBMS (database management system). Každá databáza je v MySQL tvorená z jednej alebo z viacerých tabuliek, ktoré majú riadky a stĺpce. V riadkoch sa rozoznávajú jednotlivé záznamy, stĺpce udávajú dátový typ jednotlivých záznamov, pracuje sa s nimi ako s poľami. Práca s MySQL databázou je vykonávaná pomocou takzvaných dotazov, ktoré vychádzajú z programovacieho jazyka SQL (Structured Query Language). [10]

Programovacie jazyky Knižnice pre prácu s MySQL databázami sú dostupné vo

všetkých hlavných programovacích jazykoch pomocou príslušných API funkcií. Okrem toho ODBC rozhranie s názvom MyODBC povoľuje prídavné programovacie jazyky, ktoré pomáhajú ODBC rozhraniu komunikovať s MySQL databázou, napríklad ASP alebo ColdFusion. MySQL server a oficiálne knižnice sú implementované predovšetkým v ANSI C/ANSI C++.[10]

Aplikácia MySQL je populárna pre jeho použitie vo webových aplikáciach a databázových komponentoch LAMP,MAMP, a WAMP platforiem (Linux/ Mac/ Windows-Apache-MySQL-PHP/ Perl/ Python), a pre jeho nástroje na hľadanie chýb ako Bugzilla, ktoré používajú otvorené zdrojové kódy. Jeho obľúbenosť vo vzťahu k tvorbe webových aplikácií je úzko zviazaná s popularitou PHP-čka a Ruby on Rails, ktoré sú často kombinované s MySQL. PHP a MySQL sú základné komponenty pre tvorbu redakčných systémov (CMS) ako napríklad Joomla!, WordPress, phpBB, Ebay alebo Drupal. Wikipédia beží na softvéry MediaWiki, ktorý je napísaný v PHP-čku a taktiež používa databázu MySQL. [10]

5.3.3 CSS

Kaskádové štýly alebo CSS (skratka z angl. Cascading Style Sheets) je všeobecné rozšírenie HTML o možnosti opisu vzhľadu textu základnými parametrami bežného DTP. Štýly umožnili oddeliť štruktúru HTML alebo XHTML od vzhľadu. [13]

CSS je skratka anglického výrazu Cascading Style Sheets, teda Kaskádové štýly. Konzorcium W3 (http://www.w3c.org) označuje CSS ako jednoduchý mechanizmus na vizuálne formátovanie internetových dokumentov. [13]

Pomocou Kaskádových štýlov je možné vytvárať štruktúrované dokumenty, teda oddeliť obsah dokumentu (HTML) od jeho vzhľadu (CSS). Získame tým najmä prehľadný a pomerne jednoduchý kód a použitím CSS v externých súboroch zmenšíme aj dátovú veľkosť jednotlivých dokumentov, uľahčíme si prácu pri prípadnej zmene vzhľadu www stránky, keď zmenením jediného súboru úplne zmeníme jej vzhľad. Ak Kaskádové štýly využijeme na formátovanie stránky namiesto zastaralého a nevhodného spôsobu využívajúceho tabuľky, vyhneme sa tak tzv. ladeniu www stránky v rôznych prehliadačoch, pretože ak je www stránka napísaná presne podľa špecifikácie a s využitím CSS, je zaručené, že vo všetkých prehliadačoch a na všetkých platformách bude vyzerať rovnako. [13]

5.3.4 JSON

Formát JSON (JavaScript Object Notation) je určite každému webovému vývojárovi dôverne známy. JSON má proti XML niektoré neoddiskutovateľné výhody - nie je tak "ukecaný" ako XML a jeho spracovanie na klientskej strane je veľmi jednoduché a rýchle. Načítanie dát z cudzích domén nie v prehliadačoch zakázané bezdôvodne, a ak môžeme, mali by sme sa mu vyhnúť. Napriek tomu sú situácie, kedy

sa podobným operáciám vyhnúť nedá (každopádne pri akomkoľvek vkladaní kódu či dát zo servera tretej strany je potrebné byť obozretný). Potom je na mieste zvážiť použitie uvedených variantov formáte JSON, rovnako ako pri návrhu API pre webovú službu Rozlišujeme 3 typy Ako JSON-P, JSONP-X a BISON. [14]

5.3.5 Oauth – Autorizačná metóda

Protokol OAuth umožňuje webovým stránkám alebo aplikáciám (spotrebiteľov) pre prístup k chráneným zdrojom z webovej služby (Service Provider) pomocou API, bez toho aby užívatelia museli uverejňovať svoje poverenia pre spotrebiteľa. Všeobecne OAuth vytvára voľne - uskutočniteľné a generické metodiky pre overovanie API. [15]

OAuth nevyžaduje zvláštne používateľské rozhranie alebo vzor interakcie ani určiť, ako poskytovateľ služieb pre autentifikáciu pre používateľov. Protokol sa ideálne hodí pre prípady, keď overovacie údaje sú k dispozícii u spotrebiteľov, napríklad s OpenID. [15]

OAuth si kladie za cieľ zjednotiť skúsenosti a implementáciu delegovanej overovaniu webovej služby do jediného, všeobecne - riadeného protokolu. OAuth stavia na existujúcich protokoloch a na osvedčené postupy, ktoré boli nezávisle vykonané na rôznych internetových stránkach. Otvorený štandard, podporovaný veľkými i malými poskytovateľmi je podobný, presadzuje konzistentnú a spoľahlivú prevádzku, ako pre vývojárov aplikácií a používateľov týchto aplikácií.[15]

5.3.6 AppID, Consumer Key

Sú to jedinečné identifikačné čísla u poskytovateľa autentifikácie. Pod týmto unikátnym číslom je zaregistrovaná aplikácia . Pomocou tohto čísla je zabezpečená, že užívateľ bude používať aplikáciu vytvorenú pre autentifikáciu. Tento ID je hneď po vytvorení spojenia medzi aplikáciou a poskytovateľom autentifikácie uložený do request-tokenu. Na strane poskytovateľa autentifikácie je vyčítané s tokenu a je pridelené API aplikácia (application programming interface) patriaci k AppID. Toto App ID je prítomný až do konca autentifikačného dialógu. [16]

5.3.7 AppSecret

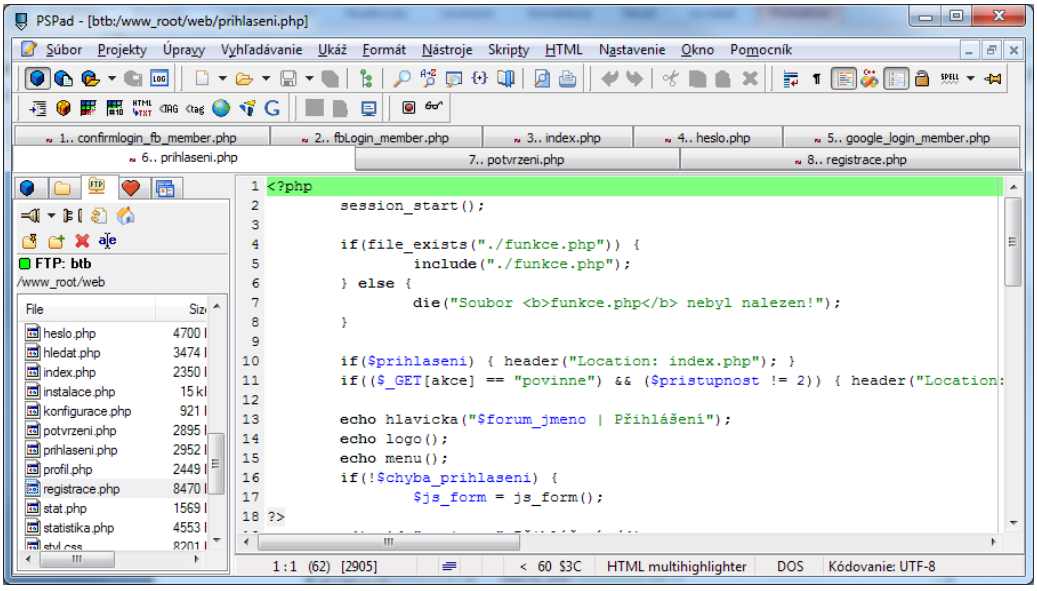
Je to tajný kľúč ktorý je šifrovaný . A je to pre šifrovanie a dešifrovanie správ počas dialógu pri prihlásení. Kľúč je zašifrovaný symetricky. Tento kľúč pozná len webová aplikácia na strane užívateľa a API aplikácia na strane poskytovateľa autentifikácie. V tajnom - kľúčovom kryptografickom režime, je jediný kľúč ktorý slúži na šifrovanie dát. Tajný kľúč môže byť v rukách jednej osoby alebo vymieňaný medzi

odosielateľom a príjemcom správy. [16]

Tajné - kryptografické kľúče sa používajú na odosielanie tajnej správy medzi dvoma stranami. Odosielateľ aj príjemca musia mať kópiu tajného kľúča, ale môže byť ohrozená strata kľúča počas prepravy. Ak je potreba, je možné dať vopred tento kľúč príjemcovi, ale nemusí byť časťou správy a tým je zaistená ešte väčšia bezpečnosť. Pri zachytenej správy nežiadaný príjemca nevie dešifrovať správu bez kľúča . Avšak, keď je potreba poslať šifrovanú správu niekomu, komu nebol zverejnený kľúč, bude treba vymyslieť si spôsob, ako vymeniť kľúče bezpečným spôsobom. Jednou z metód je poslať cez ďalší zabezpečený kanál, ale toto môže byť riskantné v niektorých prípadoch. [16]

5.3.8 PSPad

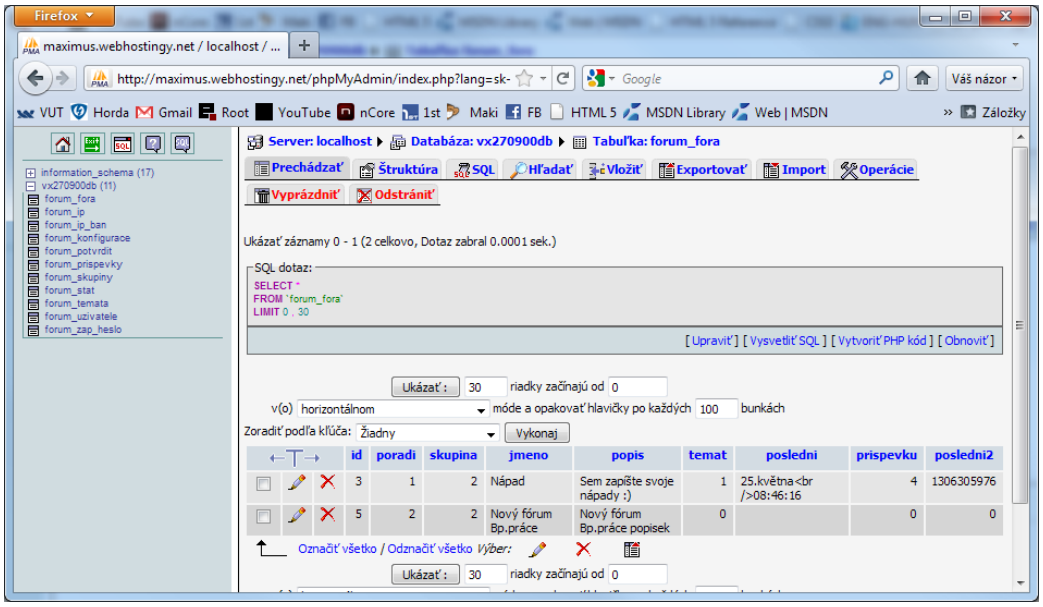
PsPad je textový editor používaný predovšetkým na vývoj webových stránok. Program poskytuje radu funkcii pre uľahčenie písania html stránok, php skriptov či css štýlov. dokáže pracovať až s 30 jazykmi (napr. PHP, HTML, XML, ASP, SQL ...) Jeho funkcie a užívateľské prostredie je orientované veľmi intuitívne a funkčne. Program obsahuje FTP klient, zvýrazňovanie syntaxu, HEXa editor s vkladaním, HTML Tidy - validátor, ukážku webu pri práci a mnoho ďalších funkcií. Pri začínaní nových projektov je možné využiť šablónu. Program disponuje aj veľmi kvalitne spracovanou pomocou. V podstate sa jedná o jednoduchý editor, ktorý práve vďaka tejto vlastnosti získal veľkú popularitu.



Obrázok 5.1: PSPad.

5.3.9 phpMyAdmin

PhpMyAdmin je nástroj napsaný v PHP, určený pro administraci MySQL serverů pře webové rozhraní. Umožňuje tvorbu a odstranění databází a tabulek, rušení, přidávání a editaci datových polí, spouštění libovolných SQL příkazů, správu klíčů polí, správu privilegií, export dat v různých formátech. Vyžaduje PHP verze 5.2+ a MySQL 5.0+.[10]



Obrázok 5.2: phpMyAdmin

5.4 Vytvorenie fórumu

Pri tvorbe fórumu som použil technológie PHP ,CSS, JSON na výmeny a spracovanie dáta a formulárov.

Ďalším krokom pri tvorbe mojej webovej stránky bol návrh a implementácia relačnej databázy pre obsluhu fórumu. Ktorá je umiestnená na platenom doméne. V mojom prípade som mohol využiť možnosť používať firemnú doménu.

`http://www.btbsro.sk/web/`

Integrované pracovné prostredie pre databázový systém nie je možno používať, lebo pri registrácie aplikácie u poskytovateľa autentifikácie, musíme zadať URL pre doménu kde chceme použiť službu.

Zrdojový kód pre môj web je uvedená na CD prílohe.

5.5 Single Sign – On pre Facebook

V poslednej dobe sa do ponuky systémov zdieľaného prihlásenia k webovým službám pridali silní hráči, ktorí sa doteraz na prvý pohľad míňali. Svoje systémy predstavili krátko po sebe hneď tri významné firmy: Google Friend Connect, MySpace Dáta Availability a Facebook Connect.Ale časovo sa pridali aj firmy, ako Yahoo, Twitter, WindowsLive .

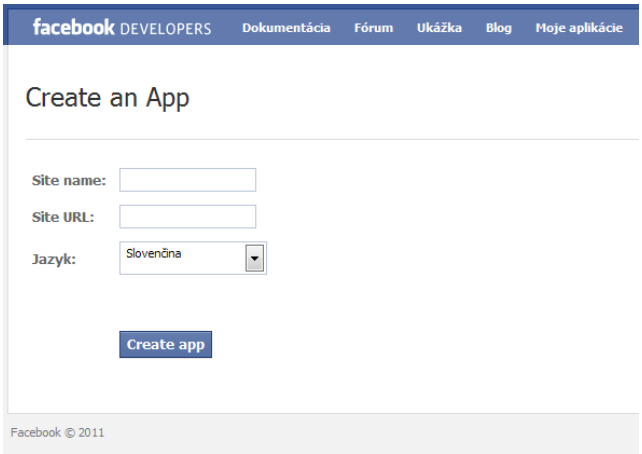
Facebook je digitálna sociálna sieť, ktorá sa zrodila na Harvardovej univerzite v roku 2004 ako komunitný portál. Hlavná myšlienka Facebooku je veľmi jednoduchá a v tom je pravdepodobne ukryté aj tajomstvo jej úspechu. Facebook ako digitálna sociálna sieť umožňuje svojim užívateľom aktívne udržiavanie osobných kontaktov, vzájomné zdieľanie myšlienok, pocitov a zážitkov s priateľmi a známymi nech sú kdekoľvek na svete.Facebook tak od základov zmenil pohľad na udržiavania starých a vytváranie nových osobných vzťahov a ešte viac prehĺbil prepojenie súkromného života s internetom.

5.5.1 Registrácia aplikácie u Facebook

Je nutné zaregistrovať svoj web na Facebook a dostať AppID. AppID je jedinečný identifikátor pre webovú aplikáciu, ktorý zabezpečuje, že je správna úroveň zabezpečenia v mieste medzi užívateľom a webovej stránky. Zaregistrovať svoj web je možno na adrese:

`https://developers.facebook.com/setup/`

kde zadáme meno aplikácie (Site name) a doménu (Site URL) pre ktorú chceme aplikáciu registrovať a ešte si zvolíme jazyk aplikácie.



Obrázok 5.3: Registrácia aplikácie u Facebook

5.5.2 Autentifikácia pomocou Oauth 2.0

Facebook pomáha zjednodušiť a zlepšiť registráciu a prihlásenie užívateľov a pomocou prihlasovacieho systému Facebooku. Užívatelia nemusia vyplniť ešte jeden registračný formulár alebo si pamätať iné užívateľské meno a heslo pre použitie webových stránok. Tak dlho, kým užívateľ je podpísaný do Facebooku, sú automaticky prihlásený do webových stránok rovnako. Použitie Facebook pre prihlásenie vám poskytne všetky informácie, ktoré potrebujete pre vytvorenie sociálne, osobné skúsenosti od okamihu, keď používateľ navštívi vaše stránky v prehliadači. [16]

Facebook Platform využíva OAuth 2.0 pre autentifikáciu a autorizáciu. Aj keď sa môžete prihlásiť na webové stránky pomocou OAuth 2,0 priamo, voľne šíriteľný JavaScript SDK je najjednoduchší spôsob, ako využiť Facebook pre prihlásenie. [16]

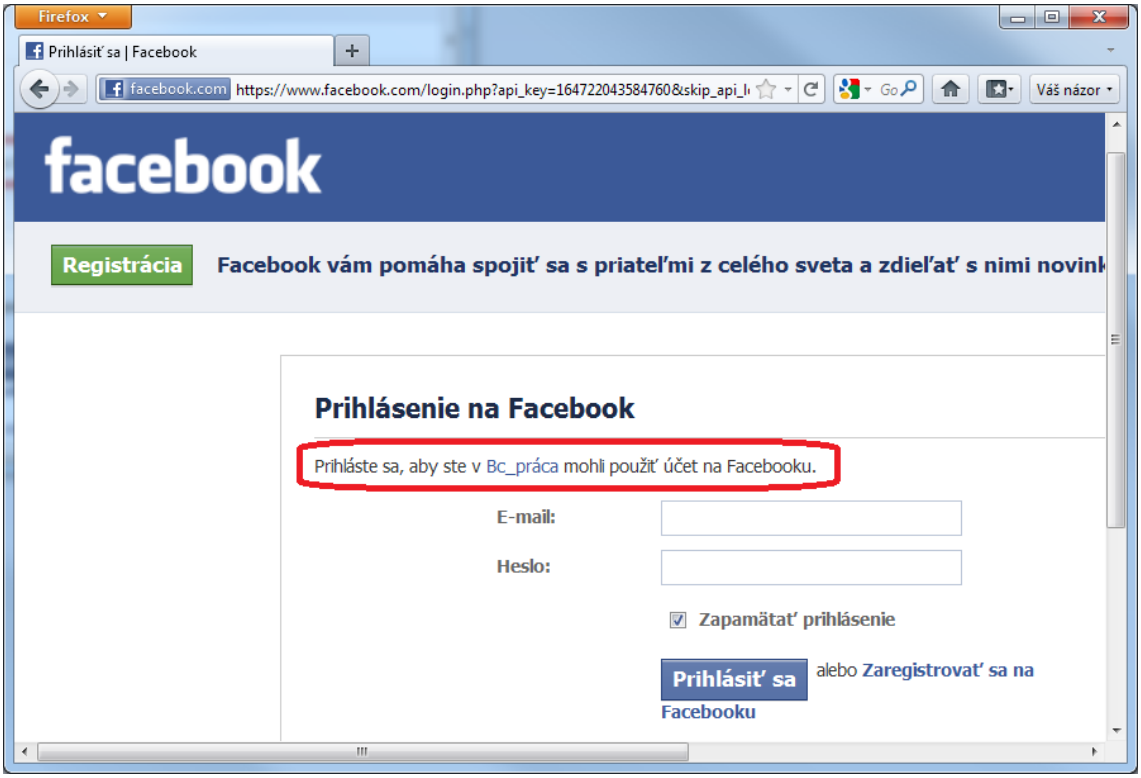
Pre prihlásenie užívateľa do stránky, je potreba stanoviť tri veci. Po prvé, Facebook potrebuje overenie užívateľa. Používateľ sám seba prezradí, že kto vlastne je a to s pomocou prihlasovacieho systému Facebooku. Užívateľ je presmerovaný na Sing-on dialóg, kde zadá svoje prihlasovacie údaje. Potom Facebook potrebuje overiť webové stránky. To zaisťuje, že používateľ dáva svoje informácie na stránkach odkiaľ chce prihlásiť. Napokon, používateľ musí explicitne povoliť webové stránky pre prístup k ich informáciám. To zaisťuje, že používateľ vie presne, aké súkromné dáta sú oznámené na webovej stránke. [16]

V tomto bode bude z webovej aplikácie uživateľ presmerovaný na Facebook kde overí sám seba. Príklad request-tokenu v URL pre aplikáciu s názvom "Bc.práca" ktorá beží na http://www.btbsro.sk/web/ :

```
http://www.facebook.com/dialog/oauth?client_id=164722043584760&redirer
e_uri=http://www.btbsro.sk/web/confirmlogin_fb_member.php
&client_secret= bec161fd0c65f0fe738f8006b724b8c9&scope=email
```

`http://www.facebook.com/dialog/oauth?` Ukazuje na adresu kde bude prebiehať dialogové okno medzi užívaľom a poskytovateľom autentifikačnej služby v tomto prípade na Facebook. Parameter `client_id` reprezentuje ID aplikácie (AppID). `Redirect_uri` reprezentuje URL kam po overení uživateľa musí presmerovať Facebook. V client_secret je uložený Secret Key s pomocou ktorého sú šifrované a dešifrované dáta. `Scope` znázornuje požiadavek na údaje, ktoré budú po prihlásení dostupné o užívateľovi.

Obrázok 5.4 znázornuje prihlasovacý dialóg na ktoré bol užívateľ presmerovaný. Tu užívateľ zadá svoje prihlasovacie údaje aby bol overený u Facebooku.



Obrázok 5.4 Facebook login dialóg

Pri úspešnom prihlásení, Facebook pošle naspäť návratový kód na portál kam chce užívateľ dostať. V kódu je uložený id užívateľa, ktorý dostal prístup k aplikácie, súhlas pre autorizáciu a čas pre ktorý bude aktívne spojenie ešte pred autentifikáciou.

V ďalšom kroku portál s prijatým návratovým kódom môže žiadať o autentifikácie uživateľa. Ktorý uvede pomocou URL:

```
http://www.facebook.com/dialog/access_token?client_id=164722043584760&
redirere_uri=http://www.btbsro.sk/web/confirmlogin_fb_member.php
&client_secret=bec161fd0c65f0fe738f8006b724b8c9&code=WIA0zBOEDg44QrRtP
qOdeQQg.eyJpdiI6IlBhTVZUSWUtS1pmVWZsQjJqZUJERXcifQ.r5KjXToyR5q4Day2c3g
ZrZlqrjmnVqbntuV1bxk1jAb17fYIIBTjZOiGo67b1QO0PJpO22RIVaojss8NyeEgMKRAH
h744WDjjVq75CEiFJOCebfucezJG62E2rXep4i5
```

Kde nový parameter `code` reprezentuje autorizačný kód pre overení užívateľa na Facebooku. Pri preposlanie tohoto kódu v URL Facebook overí, že užívateľ je registrovaný a má prístup k Facebooku.Po overení Facebook pošle naspať potvrdzovací access_token v ktorom je schválený užívateľ a portál môže použiť údaje o užívateľovi..

V poslednom kroku aby portál dostal všetky informácie a neobdržal len overený ID užívateľa môže poslať žiadosť pre užívateľské údaje pomocou URL:

```
https://graph.facebook.com/me?164722043584760|2.AQDQvCejEbHPAmJ3.3600.
1306746000.1-1763899293|15qRWknEqf5zXRW7JWLmN5wmz64&expires=4217
```

Na túto žiadosť Facebook pošle naspäť jeden JSON objekt, v ktorom sú uložené informácie o užívateľovi. Je to prospešný, keď chceme uložiť údaje o návštevníkovi portálu, alebo po prihlásenia vypísať meno pod ktorým je prihlásený.

Objekt môže vypadať takto:

```
$temp_user=Username{"id":"1763899293","name":"EndreTak\u00e1cs","first
_name":"Endre","last_name":"Tak\u00e1cs","link":"http:\/\/www.facebook
.com\/endre.takcs","username":"endre.takcs","birthday":"07\/12\/1989",
"hometown":{"id":"103765512994899","name":"Nov\u00e9Z\u00e1mky"},"loca
tion":{"id":"107645375935528","name":"Brno,CzechRepublic"},"gender":"m
ale","email":"endre.takcs\u0040gmail.com","timezone":2,"locale":"sk_SK
","languages":[{"id":"109189675767281","name":"Hungarian"},{"id":"1066
33689373139","name":"Slovencina"},{"id":"106059522759137","name":"Engl
ish"}],"verified":true,"updated_time":"2011-05-19T08:01:27+0000"}
```

A spomocou funkcie `json_decode()` môžeme získať údaje z objektu na ďalšie použitie.

```
$user = json_decode($temp_user);

$name = $user->name;

$email = $user->email;

$fb_id = $user->id;
```

5.6 Single Sign – On od ostatných firiem

V dnešnej dobe okrem Facebooku prijali myšlienku Single Sign – On aj Google, Yahoo, MySpace, Twitter a ešte možstvo veľkých firiem. Tieto firmy vkladajú veľký dvôraz na vyvíjanie webových aplikácií, aby patrili medzi najpopulárnejších webových portáloch. Vkladajú množstvo peniazov a úsilí aby splnili požiadavky uživateľov.

Pri samostatnom vývoji každý portál má svoje výhody i nevýhody a majú rozdieľ aj v množstve poskytnutých aplikácii, ale aj rozlíšia aj v ako implementovať aplikácie na strane klienta. Počas skúmania rôznych velkých firiem pre možnosť implementácie ďalšieho prihlasovaciemu systému som zistil rozdiely používané v službách:

- Google a WindowsLive nemá možnosť pre samotné využívanie služby OAuth. Je potreba implementovať Single Sign – On pomocou OpenID + OAuth dvojíc.
- Twitter a Yahoo povoluje používanie samotného systému OAuth ale je programátorské náročnejšie, vyžaduje znalosť XML jazyka. Ale pomocné dokumentácie pre vyvíjanie nie sú dostupné v dostatočnom miere. A vývoj je ťažkopádny.

5.7 Inštalácia navrhnutého portálu

Na CD prílohe sú uložené zdrojové kódy a pomocné editačné programy pre prevádzkovanie webového portálu. Záujemca podľa nasledujúcich bodov môže nastaviť pre vlastné používanie:

- Na vašej doméne do koreňovej složky nakopírujte rozbalené súbory z archívu portal.zip, ktorá je na CD prílohe. Je možno prevádzkovať aj na subdoméne, ale pri tom v koreňovej složke vytvorte složku (napr. Portal/) a potom do nej kopírujte súbory z archívu.
- Editujte súbor konfigurace.php a nastavte v ňom prihlasovacie údaje k vašej databáze.

```
$db_server = "menodatabázy";
$db_login = "loginname";
$db_heslo = "heslo";
$db_jmeno = "meno";
```

- V prehliadači spustiťe súbor instalace.php (napr. www.vasweb.sk/instalace.php). PHP script v tomto súbore vytvorí všetky tabuľky v databáze pre správnu funkčnosť.
- Teraz je už portál pripravené na použitie. (www.vasweb.sk/index.php)
- Pre prvý vstup do administrácie používajte následujúce údaje :

  Prihlasovacie meno: Admin

  Heslo: Heslo

- Po vytvorení účtu cez vyššie uvedení účet môžete prideliť administrátorské práva pre vlastní účet pod menu Práva v administrátorskom sekcii.
- Pre nastavenie AppID a AppSecret vlastného Single Sign – On apikácie poskytované z Facebooku je možnosť nastaviť pod administrátorský účet pod sekcii Konfigurace.

6 ZÁVER

V rámci bakalárskej práce bola popsaná oblasť jednotného prihlásenia na úrovni teórii. Boli zhrnuté základné teoretické poznatky, z ktorých čitateľ dozvie o funkciách jednotného prihlásenia, ďalej jej štruktúry, zabezpečeniu a autentizačné pomôcky používané v tejto oblasti. V práce je opis aj na Single Sign-On vo systému Windows. Sú tu uvedené výhody, domény a zabezpečovacie mechanizmy.

Druhá časť zameriava na rozbor Web Single Sign-On a návrh praktickej časti bakalárskej práce. Pri rozbore je popsaná autentifikačný systém pomocou tretej strany, jednotlivé vyskytujúce moduly a ich práva a účel v systéme. Podľa získaných informácií je potom realizovaná praktická časť s formou webového portálu s vlastnosťami ako fórum. Ďalšie informácie získané počas vývoja boli pridané k časti riešenia SSO aplikácie.

Celý webový systém bol navrhnutý z cieľom vytvoriť systém pre prezentáciu Single Sign – On, a pre ktorý bude možné naprogramovať ďalší modul, takže v budúcnosti systém by rozšírili modulom plniaci úlohu autentifikácie pomocou tretej strany. Napríklad by sa v budúcnosti mohol vytvoriť modul pre pirhlásenie pomocou Yahoo alebo Twitter, ktoré podporujú Oauth autentifikačný mechanizmus, ale vývojár mal by ešte iplementovať jazyk XML. Pre Google a WindowsLive je nevhodné, lebo by bolo treba prerobiť databázový systém kvôli OpenID.

LITERATÚRA

[1] Preliminary Specification. X/Open Single Sign-on Service (XSSO)— Pluggable Authentication Modules [online]. United Kingdom : The Open Group, 1997 [cit. 2010-12-09]. Introduction to Single Sign-on, s. . Dostupné z WWW: <https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=p702>. ISBN 1-85912-144-6.

[2] Microsoft. Understanding Enterprise Single Sign-On [online]. 2010 [cit. 2010-12-09]. Understanding Enterprise Single Sign-On. Dostupné z WWW: <http://msdn.microsoft.com/en-us/library/aa745042(BTS.10).aspx>.

[3] Microsoft. Single Sign-On in Windows 2000 Networks [online]. 2010 [cit. 2010-12-09]. Single Sign-On in Windows 2000 Networks. Dostupné z WWW: <http://technet.microsoft.com/en-us/library/bb742456.aspx#XSLTsection125121120120>.

[4] Microsoft. So What Is Active Directory? (Windows) [online]. 2010 [cit. 2010-12-09]. So What Is Active Directory?. Dostupné z WWW: <http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx>.

[5] MIT Kerberos. Kerberos: The Network Authentication Protocol [online].[cit. 2010-12-09]. Kerberos: The Network Authentication Protocol. Dostupné z WWW: <http://web.mit.edu/kerberos/>.

[6] Public key infrastructure. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 09.March.2003, last modified on 16.December.2010 [cit. 2010-12-17]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Public_key_infrastructure>

[7] Springer. World Wide Web [online]. 2010 [cit. 2010-12-09]. World Wide Web. Dostupné z WWW: <http://www.springer.com/computer/database+management+%26+information+retrieval/journal/11280>.

[8] AES [online].[cit. 2010-12-17]. AES - nový šifrovací standart. Dostupné z WWW: <http://www.kryptografie.wz.cz/data/aes.html>.

[9] KONÍČEK, Tomáš. LDAP [online].[cit. 2010-12-09]. LDAP. Dostupné z WWW: <http://www.fi.muni.cz/~kas/p090/referaty/2007-jaro/ct/ldap.html>.

[10] KOFLER, Michael ; ÖGGL, Bernd. PHP5 a MySQL5. Brno : Computer Press, a.s., 2007. 608 s.

[11] LUKEŠ, Dan. *HTTPS - bezpečnost jen pro vyvolené? - Lupa.cz* [online]. 2001 [cit. 2010-12-09]. HTTPS - bezpečnost jen pro vyvolené?. Dostupné z WWW: <http://www.lupa.cz/clanky/https-bezpecnost-jen-pro-vyvolene/>.

[12] CESNET. Technicka zprava - WebISO, Single Sign-On řešení pro WWW [online]. 1996 [cit. 2010-12-09]. Technicka zprava - WebISO, Single Sign-On řešení pro WWW. Dostupné z WWW: <http://www.cesnet.cz/doc/techzpravy/2005/webiso/>.

[13] CROFT, Jeff, LLOYD, Ian, RUBIN, Dan. Mistrovství v CSS - Pokročilé techniky pro webové designéry a vývojáre, Brno : Computer Press, a.s., 2008.

[14] *JSON* [online]. 2010 [cit. 2011-05-27]. Úvod do JSON. Dostupné z WWW: <http://www.json.org/json-cz.html>.

[15] *OAuth Community Site* [online]. 2010 [cit. 2011-05-27]. OAuth. Dostupné z WWW: <http://oauth.net/>.

[16] *Facebook Developers* [online]. 2011 [cit. 2011-05-27]. Apps on Facebook.com. Dostupné z WWW: <https://developers.facebook.com/docs/guides/canvas/>.

ZOZNAM SKRATIEK

SSO	Single Sign-On
WebSSO	Web Single Sign-On
RACF	Resource Access Control Facility
PKI	Public Key Infrastrukture
ID	Identifikation
CA	Certifikation Authority
PMI	Privilege Managment Infrastructure
OTP	One – Time Password
TFA	Two – Factor Authentication
SNA	System Network Architecture
AD	Active Directory
KDC	Key Distribution Center
TGT	Ticket Granting Ticket
ST	Service Ticket
PC	Personal Computer
SID	Security Identification
ID	Identification
MMC	Microsoft Managment Console
LDAP	Lightweight Directory Access Protocol
HTTP	Hyper Transfer Protocol
WWW	World Wide Web
HTTPS	Hyper Transfer Protocol Secure
AES	Advanced Encryption Standard
URL	Uniform Resource Locator
PHP	Hypertext Preprocessor
MySQL	My Structured Query Language
CSS	Cascading Style Sheets
JSON	JavaScript Object Notation
AppSecret	Application Secret
AppID	Application ID

ZOZNAM PRÍLOH

1 ks CD