Jednotný autentifikačný systém na Univerzite Komenského

Unified Authentication at Comenius University

Peter KOPÁČ – Matej ZAGIBA – Pavol MEDERLY

Abstract
This paper is concerned with the authentication solution at Comenius University. Among its chief advantages is the containment of client credentials to the central log-in server only. This means that the application servers themselves never come into contact with the authentication data, thus improving overall security of the solution. We will present the architecture and exclusively open-source technology used in our solution (CoSign, Kerberos, LDAP), as well as the methods used for integrating our authentication architecture with other IT systems in use at Comenius University.

Keywords
authentication, security, single sign-on, CoSign, integration

Úvod

Problematika digitálnej identity si v dnešnom svete vyžaduje čoraz väčšiu pozornosť. Bežný používateľ prichádza pri každodennej práci do kontaktu s mnohými systémami vyžadujúcimi autentifikáciu. Používateľ potom často zbytočne opakuje ten istý autentifikačný úkon viackrát, pretože jednotlivé systémy spolu nekomunikujú. Tomuto sa dá správnym využitím dostupných technológií zabrániť a tak zvýšiť nielen efektivitu, ale aj bezpečnosť práce.

Tieto problémy sú v súčasnosti aktuálne aj na Univerzite Komenského. Ich riešením sa zaoberá projekt *Jednotný autentifikačný systém (JAS) UK*. Cieľom projektu je vytvoriť systém, ktorý odbremení používateľov od nutnosti pamätania si veľkého množstva prístupových hesiel a umožní centralizovanú správu používateľov a ich hesiel.

Jednotná autentifikácia – výhody a nevýhody

Výhody poskytované jednotným autentifikačným riešením sú neodškriepiteľné. Používateľovi odpadá nutnosť pamätať si mnoho hesiel a prípadnú zmenu hesla vykoná na jednom mieste. Správcovia jednotlivých systémov zapojených do jednotného riešenia ocenia sprehľadnenie správy používateľov a znížený počet problémov súvisiacich so zabudnutými heslami.

Centralizácia však so sebou nesie aj riziká – prezradenie jednotného hesla je závažným bezpečnostným incidentom, rovnako ako nedostupnosť autentifikačnej služby. Navyše, vzhľadom na to, že jednotlivé aplikácie sú rôzne významné z pohľadu bezpečnosti (napr. aplikácia na vyplácanie štipendií v porovnaní s prístupom k elektronickej pošte), niekedy má význam používať viaceré heslá – tak, aby napríklad pri prezradení hesla k elektronickej pošte pri práci v internetovej kaviarni nebola ohrozená bezpečnosť ostatných aplikácií. Tieto nevýhody treba mať na pamäti pri výbere použitých technológií a návrhu architektúry riešenia.

Najbežnejšie používané riešenie problematiky jednotnej autentifikácie spočíva vo využití jedného adresára LDAP (Lightweight Directory Access Protocol), v ktorom sú uložené

autentifikačné údaje používateľov. K tomuto adresáru sa pripájajú jednotlivé služby na to, aby overili autentifikačné údaje, ktoré dostanú od používateľa. Tento prístup má však niekoľko závažných slabín.

Pravdepodobne najzávažnejšou slabinou tohto riešenia je skutočnosť, že používateľ musí svoje autentifikačné údaje odovzdať službe, aby ju táto mohla overiť voči LDAP. Tým vzniká riziko – používateľove autentifikačné údaje sú iba natoľko bezpečné ako bezpečná je najmenej zabezpečená služba. Zapojením jedinej málo dôveryhodnej služby preto zásadne utrpí bezpečnosť všetkých pokrývaných služieb.

Ďalším problémom je fakt, že služby musia mať priamy prístup k LDAP. Tento prístup, akokoľvek obmedzený, predstavuje bezpečnostné riziko.

Používané riešenia navyše často nie sú skutočnou jednotnou autentifikáciou, pretože používateľ zadáva svoje autentifikačné údaje pri prístupe ku každej z aplikácií – ide teda iba o jednotný login. Na dosiahnutie skutočnej jednotnej autentifikácie je nutné použiť ďalšie architektonické vrstvy, často komerčného charakteru.

Riešenie, ktoré sme použili v rámci projektu JAS, odstraňuje všetky tieto spomínané nevýhody. Ako úložisko autentifikačných údajov sa používa Kerberos, ktorého protokol je špeciálne navrhnutý tak, aby heslo používateľa nikdy nemuselo opustiť jeho lokálny stroj. V prípade webových služieb rolu lokálneho stroja zastáva dôveryhodný centrálny server. Používateľ teda musí svoje autentifikačné údaje zveriť len centrálnemu serveru. Ďalej sa už tieto údaje nedostanú.

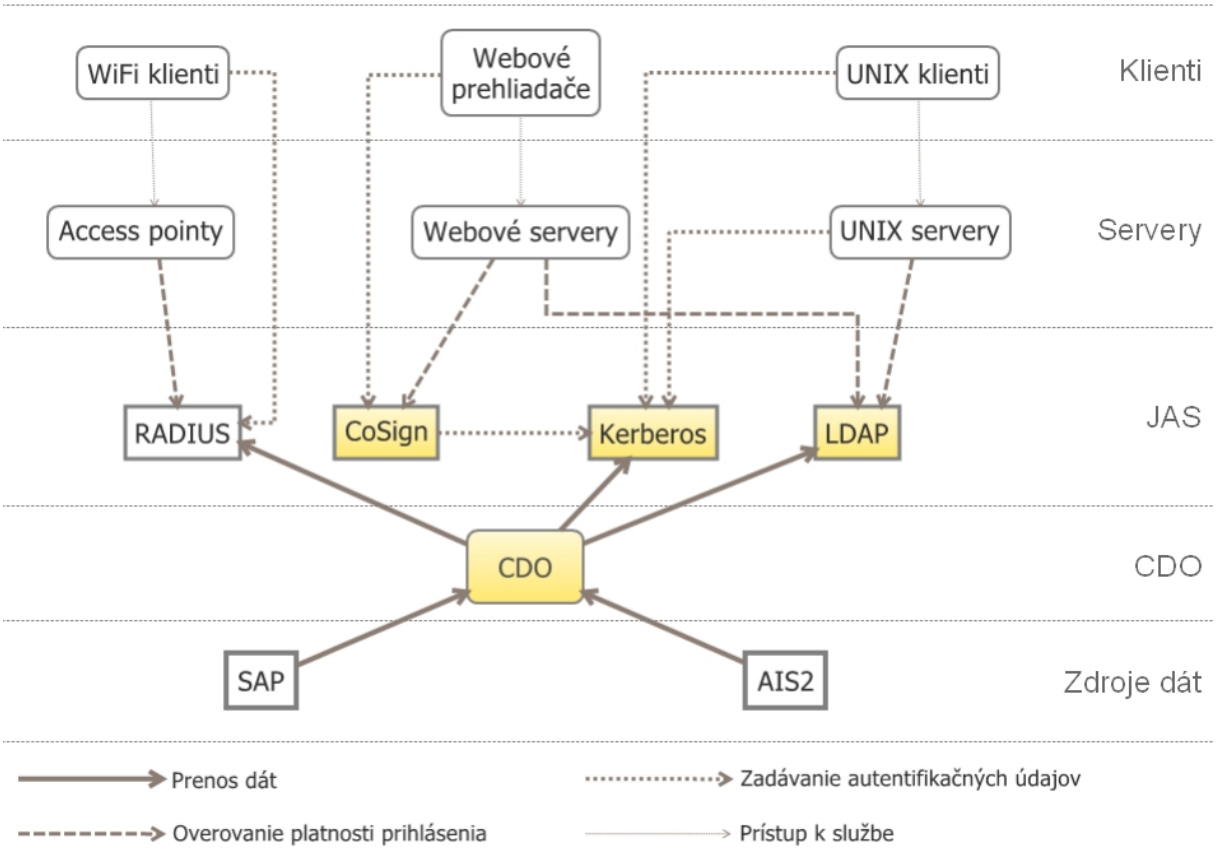
Zapájanie málo dôveryhodných služieb taktiež neohrozí celkovú bezpečnosť architektúry, pretože autentifikáciu vykonáva centrálny server, ako je detailne popísané nižšie. Málo dôveryhodná služba tak nemá prístup k údajom, ktoré by mohla potenciálne zneužiť. Pritom je naše riešenie skutočnou jednotnou autentifikáciou – používateľ sa prihlasuje iba raz a toto prihlásenie platí do všetkých pokrývaných služieb.

Architektúra riešenia

Architektúra jednotného autentifikačného systému (obr. 1) pozostáva zo špecializovaných systémov, ktoré navzájom komunikujú. Na najnižšej vrstve schémy sú systémy, ktoré sú zdrojom osobných údajov (akademický informačný systém – AIS2, personalistika – SAP). Tieto údaje sa v centrálnej databáze osôb (CDO) zhromažďujú, kontrolujú a poskytujú ďalším odberateľom. V strede schémy je jednotný autentifikačný systém (JAS), ktorý zahŕňa Kerberos, LDAP, RADIUS a CoSign a poskytuje autentifikačné a adresárové služby koncovým systémom. Tieto služby používajú koncové systémy a klienti, ktorí sa k nim pripájajú. Koncové systémy môžu byť veľmi rôznorodé – od samotného AIS2 (na účely autentifikácie používateľov), cez ľubovoľné webové servery a webové aplikácie, ktoré sú na nich prevádzkované, až po špecializované UNIX-ové servery. Jednotlivé pracovné stanice prípadne webové prehliadače, ktoré koncový používateľ používa na prístup k službám sa na schéme nachádzajú na najvyššej úrovni.

Vzhľadom k rôznym bezpečnostným požiadavkám koncových systémov a technologickým obmedzeniam JAS používa niekoľko úrovní hesiel. Tzv. L0 („level 0“) heslo je najslabším autentifikačným mechanizmom, ktorý je určený na použitie v bezpečnostne menej

významných službách či službách, kde sa predpokladá jeho zapamätanie v klientoch (potenciálne aj vo forme otvoreného textu). Toto heslo si používateľ sám nemení, pri podozrení na jeho prezradenie však môže byť vygenerované nové. Najčastejším použitím je prihlásenie sa do univerzitnej virtuálnej privátnej siete (VPN), k univerzitnému proxy serveru sprístupňujúceho platené elektronické informačné zdroje z prostredia mimo UK, či k bezdrôtovým prístupovým bodom EduRoam.



Obrázok 1: Architektúra jednotného autentifikačného systému

Najpoužívanejším mechanizmom je L1 („level 1“) heslo. Toto heslo si môže používateľ ľubovoľne nastaviť a je považované za dostatočný dôkaz o používateľovej identite, preto práca s ním podlieha prísnym pravidlám, napr. na jeho zmenu v prípade zabudnutia je vyžadovaná osobná návšteva zodpovedného pracovníka používateľom (v prípade, že máme k dispozícii používateľom overené mobilné telefónne číslo, môže si v prípade zabudnutia L1 heslo nechať poslať nové formou SMS správy).

Posledným druhom hesla je L2 heslo (tzv. bezpečnostný kód). Toto heslo potrebuje iba malá časť používateľov, je totiž vyžadované pri prístupe k bezpečnostne kritickým údajom (v súčasnosti ide o prístup k cudzím osobným údajom v centrálnej databáze osôb). Používa sa spolu s L1 heslom ako dodatočné overenie identity používateľa.

Centrálna databáza osôb

Kľúčovou časťou systému je centrálna databáza osôb. CDO uchováva údaje o všetkých osobách, ktoré majú akýkoľvek vzťah k univerzite – zamestnanci, študenti, absolventi, externí

prednášajúci a podobne. Údaje sa do CDO prenášajú automaticky z jednotlivých zdrojových systémov. Vďaka použitej technológii, tzv. podnikovej zbernici služieb (Progress Sonic ESB [1]), sa zmena údajov v CDO prejaví prakticky ihneď po vykonaní zmeny v zdrojovom systéme – pri zmene údajov o študentoch v akademickom informačnom systéme (AIS2) okamžite, pri zmene údajov o zamestnancoch v personalistike (SAP) do 15 minút.

Do CDO sa okrem osobných informácií prenášajú aj informácie potrebné na priradenie rolí jednotlivým osobám (napr. to, že osoba XYZ je externý študent 2. ročníka doktorandského štúdia odboru aplikovaná informatika). Všetky tieto údaje vrátane notifikácií o zmenách v nich sú prostredníctvom podnikovej zbernice služieb prenášané k príslušným systémom, ktoré s nimi potrebujú pracovať (napríklad univerzitné terminály, prístupový systém, stravovací systém a podobne) – vrátane jednotného autentifikačného systému, konkrétne do modulov Kerberos, LDAP a RADIUS.

Prostredníctvom CDO je v súčasnosti realizovaná aj distribuovaná správa (zabudnutých) hesiel – táto úloha je na fakultách delegovaná spravidla na študijné a IT oddelenia.

LDAP

LDAP je štandardný protokol na prístup k adresárovým službám a vďaka širokej podpore v aplikáciách a serverových službách sme sa rozhodli časť informácií z CDO replikovať do adresára LDAP. Ako konkrétnu implementáciu LDAP sme vybrali OpenLDAP, a to jednak pre jednoduchosť správy a replikácie, ale aj pre podporu autentifikácie SASL, ktorá nám umožnila zjednotiť identity systému Kerberos so záznamami v LDAP. Práve vďaka širokej podpore je LDAP mimoriadne vhodný na správu a distribúciu prístupových oprávnení podľa pridelených rolí (príslušnosti k skupine). Uveďme niektoré príklady použitia:

- Kombinácia centralizovanej autentifikácie prostredníctvom systému Kerberos s adresárom LDAP umožňuje presne určiť, ktoré skupiny používateľov (prípadne aj jednotliví používatelia, ak je to nutné) majú k danému serveru prístup, pričom je možné kombinovať celouniverzitných používateľov s lokálnymi (či už špecifickými pre danú fakultu alebo pre konkrétny server) a výsledný zoznam ďalej sprístupniť klientom (vhodné napr. pre správu učebne).

- Modul *mod_authnz_ldap* pre systém Apache umožňuje kombinovať CoSign autentifikáciu s filtrovaním podľa ľubovoľného atribútu LDAP, čím efektívne dosiahneme rolové riadenie prístupu s granularitou až na jednotlivé stránky.

- Jednoduchý niekoľkoriadkový kód v jazyku PHP dokáže skontrolovať CoSign/LDAP parametre prihláseného používateľa a podľa potreby povoliť či zakázať prístup k danému prvku na stránke (výhodné pre jednoduchšie PHP aplikácie).

- Rozšírenie *ldap_server* pre univerzitný CMS systém TYPO3 importuje používateľov a skupiny z LDAPu podľa zadaných kritérií a v kombinácii s CoSignom umožňuje detailné riadenie prístupu používateľov k stránkam a súborom zverejňovaným na univerzitnom webe.

Hlavnou úlohou LDAP v rámci projektu JAS je distribuovať informácie, ktoré aplikácie potrebujú pri vykonávaní autorizačných rozhodnutí. V našom prípade teda nejde o

autentifikačnú technológiu, jej zakomponovaním do nášho systému sa však výrazne rozšírili jeho možnosti smerom k autorizácii používateľov v jednotlivých aplikáciách.

Kerberos
Ako centrálna autentifikačná služba bol vybraný MIT Kerberos 5 na platforme Debian. Protokol Kerberos umožnuje zapojeným službám autentifikovať používateľov bez prístupu k ich heslám, iba na základe lístkov (tickets) vydávaných centrálnou autoritou. Heslá sú potrebné iba pri prvotnom prihlasovaní sa, či už na pracovnej stanici, alebo do systému CoSign – ten si od používateľa vyžiada autentifikačné údaje, ktorými sa pokúsi autentifikovať voči Kerberosu ako bežná pracovná stanica. Ak je pokus úspešný, používateľa autentifikuje.

Nakoľko na univerzite nie je väčšina pracových staníc členom žiadnej domény, prepojenie centrálneho Kerberos serveru s lokálnymi doménami Active Directory nepredstavovalo dostatočný prínos. Zapojenie UNIX-ových serverov do prostredia Kerberos je naproti tomu vo väčšine prípadov priamočiare a nepredstavuje takmer žiadnu zmenu oproti predošlému spôsobu používania. Pritom ostáva možnosť počas prechodnej doby používať staré kontá paralelne s novými, čo uľahčuje zapojenie serverov a služieb do JASu a minimalizuje nároky na používateľov. Silnou kombináciou je spojenie autentifikácie prostredníctvom systému Kerberos s autorizáciou prostredníctvom LDAP.

CoSign
Napriek tomu, že existuje riešenie umožňujúce vo webových prehliadačoch prihlasovať sa do webových služieb prostredníctvom systému Kerberos (ide o protokol *Simple Protected Negotiation* – SPNEGO), pre praktické problémy spojené s jeho nasadením sme sa rozhodli na pokrytie webových služieb projektom JAS použiť *CoSign*.

CoSign je projekt s otvoreným zdrojovým kódom, pochádzajúci z University of Michigan. Základný princíp jeho fungovania je, že aplikačný server pokrytý CoSignom príchodzieho neautentifikovaného používateľa presmeruje na centrálny server CoSign. Tu sú overené jeho údaje a je mu vydaná cookie. Následne je presmerovaný na pôvodný aplikačný server, ktorý si cez zabezpečené spojenie overí platnosť tejto cookie priamo na centrálnom serveri CoSign. Po úspešnom overení považuje aplikačný server informáciu o používateľovej identite za overenú. S touto cookie sa môže používateľ preukázať aj u inej pokrytej služby – tá si opäť cez zabezpečené spojenie overí platnosť cookie, pričom celý proces prebieha pre používateľa plne transparentne.

Druhou podstatnou výhodou systému CoSign je jednoduchosť, s ktorou je možné pridávať či modifikovať mechanizmy, používané na autentifikáciu používateľov. Pridanie mechanizmu je iba otázkou vytvorenia ľubovoľného spustiteľného súboru (bash, perl, C, …), ktorý overí jemu poskytnuté údaje ľubovoľným spôsobom (voči databáze, systému Kerberos, lokálnemu súboru, …).

Nasadenie CoSign na aplikačný server
Prvku nasadzovanému na aplikačný server sa hovorí *filter*. Jeho úlohou je kontrolovať, či bola overená identita každého používateľa, ktorý pristupuje ku chránenému zdroju (a neoprávnené prístupy zastaviť). Filter kontroluje informáciu uloženú v cookie a konzultuje jej platnosť s lokálnou databázou i centrálnym serverom CoSign.

Na stránke projektu CoSign sú k dispozícii filtre vo forme modulov pre Apache a IIS, ako aj implementácia v Jave. V rámci projektu JAS vznikla taktiež implementácia v PHP, ktorej tvorba bola otázkou iba niekoľkých hodín práce.

Záver

Projekt JAS ešte ani zďaleka nie je zavŕšený. CoSign poskytuje niekoľko veľmi zaujímavých možností ako napríklad multifaktorová autentifikácia či požadovanie reautentifikácie pri prístupe na konkrétnu webovú službu, tie však v tejto fáze projektu nevyužívame. V budúcnosti taktiež plánujeme preskúmať možnosti protokolu SPNEGO pre dosiahnutie plne automatického jednotného prihlasovania, keď bude možné na počítačoch pripojených do domény nahradiť ručné prihlásenie na server CoSign prihlásením automatickým. Navyše existuje možnosť kompletne integrovanej jednotnej autentifikácie, kde používateľovo prihlásenie sa na pracovnú stanicu (teda prihlásenie sa do domény Active Directory či prihlásenie pomocou UNIXového modulu PAM) platí ako jeho autentifikácia aj na všetky služby pokryté projektom JAS.

Abstrakt

Tento príspevok je venovaný jednotnému autentifikačnému systému na Univerzite Komenského, ktorý umožňuje bezpečnú autentifikáciu používateľov informačného systému. Charakteristickou vlastnosťou riešenia je, že aplikačné servery neprichádzajú do kontaktu s autentifikačnými údajmi používateľa a že je postavené na produktoch s otvoreným zdrojovým kódom. V príspevku predstavíme použité technológie (CoSign, Kerberos a LDAP), architektúru riešenia na UK, ako aj spôsob integrácie autentifikačného riešenia s ostatnými systémami, ktoré sa na UK používajú.

Kľúčové slová

autentifikácia, bezpečnosť, single sign-on, CoSign, integrácia

Literatúra

[1] MEDERLY, P. – PÁLOS, G. 2008. Enterprise Service Bus at Comenius University in Bratislava. In EUNIS 2008 VISION IT: Visions for IT in higher education, Aarhus University, ISBN 978-87-91234-56-9, p. 129. Dostupné aj na internete: <http://www.eunis.dk/papers/p98.pdf>

[2] NEUMAN, C. – YU, T. – HARTMAN, S. – RAEBURN, K. 2005. The Kerberos Network Authentication Service (V5). [online] RFC 4120. Dostupné na internete: <http://www.ietf.org/rfc/rfc4120.txt>

[3] SEMERSHEIM, J, 2006. Lightweight Directory Access Protocol (LDAP): The Protocol. [online] RFC 4511. Dostupné na internete: <http://www.ietf.org/rfc/rfc4511.txt>

Kontakt

Mgr. Peter Kopáč, CIT RUK, Šafárikovo nám. 6, 81806 Bratislava, č.t.: 02/592 44 965, E-mail adresa: peter.kopac@rec.uniba.sk

Recenzent: RNDr. Darina Tothová, PhD., CIT FEM SPU v Nitre