

Nedžad Imamović, dipl. ing. el. - Magistarski rad

| | |
|----------------------------|---|
| Fakultet/Akademija | FAKULTET ELEKTROTEHNIKE |
| Tip Rada | Magistarski rad |
| Kandidat, zvanje | Nedžad Imamović, dipl. ing. el. |
| Naziv Teme | Menadžment korisničkih identiteta u Web sistemima sa primjenom na rails platformi |
| Rezime/Abstract | <p>Živimo u vremenu gdje su granice između virtuelnog i stvarnog sve više nejasne. Poprilično je jednostavno saznati s kim kontaktiramo i koga on predstavlja; rukovanje, potpis, fotografija u identifikacionom dokumentu, identifikaciona značka itd., sve to ima ulogu u fizičkoj identifikaciji. U digitalnom svijetu, potreban nam je elektronski ekvivalent, tako da znamo s kim kontaktiramo i koji autoritet posjeduje. U korporativnim okruženjima, od ključne važnosti je identifikacija i kontrola načina na koji organizacija rukuje kupcima, dobavljačima, uposlenicima i ostalim koji mogu imati interakciju sa informacionim sistemom organizacije. Česta upotreba digitalnih identiteta u današnjim informacionim sistemima vodi ka povećanom interesu u području upravljanja identitetom. U zadnje vrijeme predloženi sistemi kojima je korisnik u centru, postigli su visok nivo korisničke kontrole putem mrežnih certifikata o identitetu. Ipak, usljed nedostatka centralnog autoriteta koji bi upravljao cjelokupnim sistemom zahtjeva, korisnici su odgovorni za svoje vlastite certifikate o identitetu. Dodatno, ti predloženi sistemi sa korisnikom u centru, još uvijek imaju problema sa stanovišta sigurnosti, privatnosti i systemske rapoloživosti. Upravljanje identitetom u internetskim razmjerama zahtjeva integrisani skup infrastrukturnih servisa koji omogućavaju holistički pristup definisanju i upravljanju identitetom. Ovaj specifični niz sofisticiranih alata uključuje usluge direktorija (koji uobičajeno koriste LDAP protokol), definisanje prava korisnika, delegiranu administraciju, kao i mogućnost korisničke samostalne administracije lozinki i drugih atributa. Jak autentifikacijski sistem, opšte namjene, zajedno sa kvalitetnim upravljanjem izdavanjem certifikata su takođe centralni dio boljeg sistem upravljanja identitetima. Nakon autentifikacije, organizacije i kompanije moraju povezati i sistem za upravljanje pravima pristupa kroz razne operative sisteme, aplikacije, web bazirane aplikacije sa jedinstvenim mjestom prijave, čineći upravljanje sigurnosnim politikama još jednim važnim dijelom cjelokupnog sistema. Arhitektura upravljanja identitetom je koherentan set standarda, politika, uvjerenja i upravljačkih aktivnosti unutar organizacija i kompanija, koji omogućava efikasno upravljanje identitetima. Dodatno, upravljanje identitetima je ključna komponenta svake sigurnosne strategije. Da bi bila efikasna sigurnost zahtijeva identifikaciju i autorizaciju bilo čega što pokušava dobiti pristup bilo kojem dijelu sistemu. Informacije moraju biti čuvane na siguran i povjerljiv način, kako u prenosu tako i u njihovom smještaju. U takvim scenarijima, upravljanje tehnologijom digitalnog identiteta je osnov u prilagođenju i unaprijeđenju korisničkog iskustva, zaštiti privatnosti, definisanju odgovornosti u raznim transakcijama i interakcijama, kao i pridržavanju zakonskih propisa. Digitalni identitet se može definisati kao digitalna reprezentacija informacija, koje su poznate za određenu osobu ili organizaciju. Te informacije mogu biti iskorištene u različite svrhe, a najčešća je zahtjev za potvrdom identiteta i uspostavljanje dozvola na osnovu potvrđenog identiteta. Sa rastom popularnosti web baziranih sistema kod krajnjeg korisnika, krajnji korisnici imaju svoje korisničke račune na više web servera. Korisnici moraju da kreiraju identitet za sve te web servere i da pamte korisnička imena i lozinke. Ovo vodi do potencijalnih problema, ne samo za korisnika, nego i iz sigurnosne perspektive. Za korisnika koji ima više korisničkih računa na više različitih web servera, upravljanje identitetom znači, iz „korisničke perspektive“, prevazilaženje raznih problema sa kojima se susreću, a najčešći problem jeste upravo taj, kako efikasno upravljati sa višestrukim identitetima na više web servera sa kojima kranji korisnik vrši interakciju. U ovom radu će biti prezentirane arhitekture sistema za upravljanje identitetima koje rješavaju neke od problema, putem web baziranih aplikacija, korištenjem web tehnologija, LDAP direktorija, OpenID i OAuth protokola. Implementacija u formi web aplikacije potvrđuje koncept i evaluira arhitekture sa stanovišta sigurnosti, orijentisanosti prema korisniku i performansama. Ključne riječi: Autentifikacija, Autorizacija, Digitalni identitet, Direktorij, Federativni identitet, Identitet, Upravljanje identitetom, LDAP, OAuth, OpenID, Single-Sign-On.</p> |
| Datum | 14.12.2012 |
| Predsjednik | Dr sc. Amir Tokić, vanredni profesor, - predsjednik, Uža naučna oblast „Teorija mreža i sistema“ Fakultet elektrotehnike Univerziteta u Tuzli |
| Mentor | Dr sc. Amer Hasanović, vanredni profesor, - mentor i član, Uža naučna oblast “Računarstvo i informatika“ Fakultet elektrotehnike Univerziteta u Tuzli |
| Član komisije | Dr sc. Edin Pjanić, docent, - član, Uža naučna oblast "Računarstvo i informatika" Fakultet elektrotehnike Univerziteta u Tuzli |
| Član komisije | - |
| Član komisije | - |
| Zamjenski član | - |
| Dodatni detalji i lokacija | 14. 12. 2012. godine u 12,00 sati na Steleksu Fakulteta elektrotehnike Univerziteta u Tuzli |
| Završne Odredbe | Magistarski rad može se pogledati u Sekretarijatu Fakulteta, radnim danom od 10,00 do 14,00 sati. Pristup javnosti je slobodan. |