|  |  |
| --- | --- |
|  | Zbornik radova Fakulteta tehničkih nauka, Novi Sad |

**UDK: (Upisuje redakcija, ostaviti ovaj red)**

**DOI: (Upisuje redakcija, ostaviti ovaj red)**

**INTEROPERABILNI ADAPTER ZA RAD SA BAZAMA INFORMACIONE BEZBEDNOSTI**

Aleksandar Maričić, *Fakultet tehničkih nauka, Novi Sad*

**Oblast – Elektrotehničko i računarsko inženjerstvo**

**Kratak sadržaj –** *U ovom radu istražen je način korišćenja dva različita sistema informacione bezbednosti – Microsoft Active Directory zasnovan na Windows platformi i OpenLDAP zasnovog na Linux platformi, uočene su njihove sličnosti i razlike, razvijen je, implementiran, istestiran interoperabilni adapter za rad sa ova dva sistema informacione bezbednosti koji omogućuje korišćenje administratorske i korisničke funkcionalnosti.*

**Ključne reči:** *Informaciona Bezbendost, Interoperabilnost, Adapter*

**Abstract** – In this paper the way of using two different information security system is researched *– Microsoft Active Directory based on Windows platform and OpenLDAP based on Linux platform, their similarities and differences are identified, the interoperable adapter for those two directory services was developed, implemented and tested with supporting administration and user-related functionalities.*

**Keywords:** *Information Security, Interoperability, Adapter*

# UVOD

Informaciona bezbednost jedna od ključnih komponenti za uspešan razvoj i poslovanje kompanija. U savremenim informaciono-tehnološkim rešenjima zahteva se sve veća standardizacija, integracija i interoperabilnost rešenja koja omogućuju fleksibilan i ekonomski vođen odabir *IT* komponenti kao i mogućnost što jednostavnije promene *IT* komponenti tokom eksploatacionog perioda.

Informaciono bezbednosni sistem upravlja podacima o korisnicima, njihovim ličnim podacima, grupama kojima korisnici pripadaju, pravima pristupa i entitetima koji čuvaju podatke. Postoje različite informaciono tehnološke platforme i nad njima zasnovana rešenja informacione bezbednosti. U ovom istraživanju fokus je na dva različita informaciono bezbednosna sistema – *Micorsoft Active Directory*, zasnovan na *Windows* operativnom sistemui *OpenLDAP*, zasnovan na *Linux* OS - u. Ovi bezbednosni sistemi se oslanjaju na – *Lightweight Directory Access Protocol* (*LDAP*), ali i pored toga imaju brojne razlike koje se ogledaju u različitim tipovima entiteta, atributima, načinima povezivanja entiteta i u interfejsima za pristup njihovim bazama podataka. Prilikom migracije sa jedne platforme informacione bezbednosti na drugu, ove razlike zahtevaju promenu svih linija koda koje su specifične za jednu od platformi. Što je informacioni sistem veći, to je

**NAPOMENA:**

**Ovaj rad proistekao je iz master rada čiji mentor je bio docent dr Nemanja Popović**

broj specifičnih linija veći i promena je složenija. Za jednostavnu migraciju sa jedne informaciono bezbednosne platforme na drugu, potrebno je razviti konfigurabilni interoperabilni adapter koji će lokalizovati sve pozive funkcija ka sistemima informacione bezbednosti (uključujući i one specifične) i obezbediti pristup ka njima kroz generički sloj, dok bi se odabir baze odredio postavkom konfiguracije na jednom mestu.

U ovom radu istraženi su principi funkcionisanja sistema informacione bezbednosti *Microsoft Active Directory* (AD), zasnovan na *Windows* platformi i *OpenLDAP*, zasnovan na *Linux* platformi, njihove postavke, biblioteke za pristup i za rad sa navedenim platformama. Identifikovane su funkcije i strukture podataka za rad sa navedenim sistemima, njihove sličnosti i razlike. Dizajniran je i implementiran konfigurabilni interoperabilni adapter koji omogućuje rad sa obe bezbednosne platforme kroz generički sloj, dok se odabir platforme i bezbednosnog sloja konfiguriše na jednom mestu. Definisano i postavljeno testno okruženje koje obuhvata *AD* i *OpenLDAP* serverirazvijena je testna aplikacija, kojom je verifikovan rad adaptera.

Ovaj rad je organizovan na sledeći način: u prvom poglavlju dat je uvod. Drugo poglavlje daje kratak pregled teorijskih osnova informacione bezbednosti. U trećem poglavalju predstavljeno je predloženo rešenje. Verifikacija rešenja data je u poglavlju četiri. U petom poglavlju dat je zaključak. Literatura je navedena u šestom poglavlju, a kratka biografija u sedmom.

# TEORIJSKE OSNOVE

Informaciona bezbednost predstavlja vrlo široku i multidimenizonalnu oblast jedne organizacije koja obuhvata ljude, procese i tehnologije. Osnovni cilj informacione beznednosti je da zaštiti karakteristike informacija koje imaju vrednost za organizaciju [1]: **a)** Poverljivost – zaštita pristupa podacima od neautorizovanih korisnika; **b)** Integritet – konzistentnost podataka tokom svog životnog veka; **c)** Dostupnost – mogućnost korisnika da neometano pristupa podacima i da su mu dostupni u svakom trenutku.

U ovom poglavlju dat je pregled koncepata kontrole pristupa, *LDAP* protokola, i tehnoloških rešenja *AD* i *OpenLDAP* koji su korišćeni tokom istraživanja.

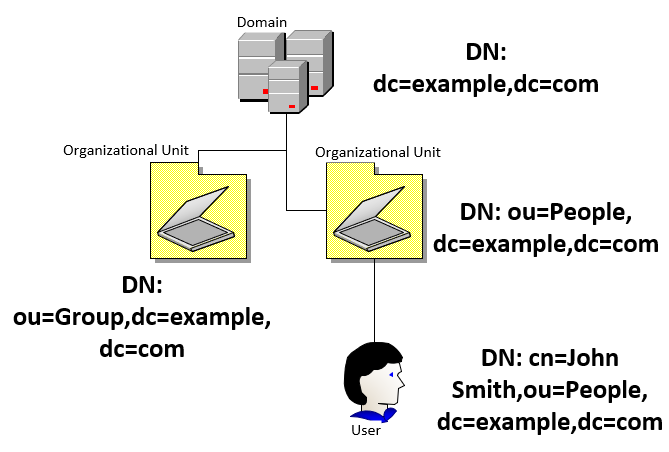
## Kontrola pristupa

Kontrola pristupa se oslanja na pojmove subjekata, objekata, operacija i dozvola da se operacija izvrši. Subjekat je entitet koji ima aktivnu ulogu u sistemu bezbednosti, dokazuje svoj identitet, pristupa objektima i inicira prenos informacija do drugih objekata ili subjekata. Subjekat može da bude: autorizovani ili neautorizovani korisnik, aplikacija, sistem ili mreža. Subjektu na nekoliko različitih načina može da se ograniči pristup objektu, a neka od tih ograničenja su: **a)** vreme pristupanja; **b)** lokacija autentifikacije subjekta; **c)** pristup van lokalne mreže; **d)** specijalna dodeljena prava pristupa. Objekat je entitet koji nema aktivnu ulogu kao subjekat. On prima ili da čuva podatke, a objekat može da bude: aplikacija, mreža, fizički prostor za čuvanje memorije, a i sam podatak može da ima ulogu objekta [2]. Operacija predstavlja vrstu obrade informacije, dok dozvole predstavljaju pravila po kojima subjekat pristupa objektu. Svaki subjekat ima listu dozvola i ta lista je definisana u listi kontrole pristupa [2].

Kontrola pristupa definiše kojim objektima subjekat sme da pristupa, kakva su njegova prava, šta korisnik sme da radi sa tim objektima. Da bi se uspostavila potpuna kontrola pristupa, subjekat mora da prođe kroz tri faze: identifikacija, autentifikacija i autorizacija. Identifikacija subjekta je njegovo predstavljanje. Autentifikacija je dokazivanje identiteta korisnika. Postoje tri načina autentifikacije subjekta [2]: **a)** Nešto što subjekat zna (npr. lozinka); **b)** nešto što poseduje (npr. hardverski uređaj); **c)** nešto što jeste, (npr. biometrijski otisak prsta). Autorizacija korisnika je mehanizam kojim se određuju privilegije subjekta i njegovi nivoi pristupa objektima. Autorizacija je moguća tek kada je subjekat identifikovan i autentifikovan. Evidentiranjem bezbednosno informacionih događajaja se prate, zapisuju i čuvaju aktivnosti na mreži u sistemu [2].

## *Lightweight Directory Access Protocol*

*LDAP* je industrijski protokol standard zasnovan na Internet Protokolu za pristup i izmenu distribuiranih podataka u bazi informacionih podataka koja čuva specifične i uređene informacije o objektima [3]. **Slog** predstavlja sve podatke o jednom entitetu. Svaki slog se sastoji od tri glavne komponente: jedinstveno ime (*Distinguished Name - DN*), objektnih klasa i atributa. Slogovi su organizovani u strukturu stabla*.* Primer *LDAP* stabla sa jednim domenom, dve organizacione jedinice i jednim korisnikom se nalazi na Slici 1. Više stabala koji su sačinjeni od slogova čine šumu. **Jedinstveno ime** je atribut kojim se na jedinstven način identifikuje svaki slog. *DN* se sastoji od relativnog jedinstvenog imena – *Relative Distinguished Name* (*RDN*) i putanje u stablu, gde se slog nalazi. **Atributi** predstavljaju osobine subjekata i objekata, imaju svoj tip i vrednost ili listu vrednosti. Slogovi se sastoje od atributa. **Klasa objekata** je specijalan atribut zajednički za slogove u bazi, jedinstveno identifikovan objektnim identifikatorom, definiše koji se atributi koriste u okviru jednog sloga.



*Slika 1* – Primer *LDAP* stabla

## *Microsoft* *Active Directory*

Predstavlja implementaciju *LDAP* protokola kompanije *Microsoft*. Prvi put je implementiran na *Windows* *2000* operativnom sistemu, a danas se koristi na *Windows Server* operativnim sistemima (poslednja verzija je *Windows Server 2019*). *AD* pruža bazu informacione bezbednosti i tehnološko rešenje kontrole pristupa koje se koriste u ovom radu. Ono omogućuje upravljanje korisnicima, grupama, organizacionim jedinicama, štampačima, aplikacijama i servisima [4]. Pored toga *AD* ima i razne druge funkcionalnosti koje prevazilaze obim ovog istraživanja.

## *OpenLDAP*

Predstavlja implementaciju bezbednosnog servisa na *Linux* operativnom sistemu. *OpenLDAP* pruža bazu informacione bezbednosti, koja može da upravlja korisnicima, grupama i organizacionim jedinicama. Osim rada sa ovim entitetima, koji spadaju u osnovnu šemu baze podataka, *OpenLDAP* pruža mogućnost proširenja šeme i samim tim se otvara mogućnost za proširenje funkcionalnosti. Prilikom instalacije *OpenLDAP* servera, inicijalno su uključene tri šeme koje obezbeđuju osnovne definicije za najčešće korišćene ekstenzije[5]:

**a)***Core.schema*;

**b)** *Cosine.schema;*

***c)*** *Inetorgperson.schema;*

## Interoperabilnost

U današnjem svetu raste potreba za složenim sistemima, koji su sačinjeni od više funkcionalnih celina. Svakom funkcionalnom celinom upravlja po jedan ili više servisa. Da bi sistem funkcionisao, a da korisnik ima osećaj kao da ga uslužuje jedan sistem, manji servisi moraju da funkcionišu skladno. Usklađenost ovih sistema je interoperabilnost. Postoje dve vrste interoperabilnosti [6]:

**a)** Sintaksna interoperabilnost –sistemi komuniciraju i razmenjuju podatke, čak iako im interfejsi ili programski jezici nisu isti.

**b)** Semantička interoperabilnost – razmenjeni tipovi podataka su razumljivi u oba sistema.

# PREDLOŽENO REŠENJE

U ovom radu je razvijen interoperabilni adapter na generičkom sloju, funkcionalan sa *AD* – om i *OpenLDAP –* om, na *Windows* i *Linux* *OS* platformama. Identifikovane su i istražene biblioteke za rad sa bezbednosno informacionim sistemima, funkcinalnostima koje nude i koje strukture podataka se koriste za razvijanje adaptera. Prilikom pokretanja adaptera se postavlja informaciono bezbednosni sistem sa kojim adapter komunicira, a izmenom na samo jednom mestu se menja komunikacija ka drugom bezbednosnom sistemu, bez dodatnih izmena u postojećem kodu. Rešenje je dizajnirano fabričkim dizajn paternom, koji od korisnika sakriva način pristupanja *AD* i *OpenLDAP* informacionim bazama podataka.

## Arhitektura sistema

Arhitektura sistema je prikazana na Slici 2. Na slici se može videti da je sistem izgrađen od sledećih komponenti: **a)** *AD* i *OpenLdap* servisi; **b)** aplikacija; **c)** konfiguracioni fajl **d)** interoperabilni adapter; **e)** log fajl.

***AD* i *OpenLDAP***su na slici prikazani kao dve baze podataka, zato što čuvaju informaciono bezbednosne podatke. Implementirana je korisnička **aplikacija**, koja je povezana sa interoperabilnim adapterom i nudi korisnicima popunjavanje podataka za kreiranje novih, izlistavanje i modifikaciju postojećih slogova, pozivajući funkcije sa interoperabilnog adaptera. **Konfiguracioni fajl** sadrži neophodne podatke za pokretanje sistema, a to su: **a)** izbor bezbednosnog servisa; **b)** naziv ciljanog domena (npr. *example.com*) **c)** *IP* adresa i port bezbednosnog sistema. **Interoperabilan adapter** je smešten na generičkom sloju i predstavlja centralnu komponentu sistema, zato što je povezan sa svim ostalim komponentama. Prilikom pokretanja sistema, iščitavaju se podaci iz konfiguracionog fajla i adapter uspostavlja konekciju sa željenim informaciono bezbednosnim servisom. Kada se uspostavi konekcija, komande se šalju sa aplikacije, do adaptera, koji ih prosleđuje do bezbednosnog servisa, koji šalje odgovor nazad do adaptera. **Log fajl** čuva zapis o poslednjem ulogovanom klijentu i vremenu kada se ulogovao.



*Slika 2* – Arhitektura predloženog rešenja

## Generički sloj

Interoperabilan adapter se nalazi na generičkom sloju, funkcionalnom na različitim platformama *OS* - a. Da bi se postigla nezavisnost od platforme na koju se oslanja sistem, rešenje je implementirano na .*NET Core* radnom okruženju koje se sastoji od procesne virtualne mašine i kolekcije klasa i sam je nezavisan je od platforme *OS* - a na koju se oslanja.

## Interoperabilnost

Za razvijanje interoperabilnog adaptera, istražene su karakteristike bezbednosnih sistema, a to su: **a)** koji interfejsi za povezivanje sa *AD* i *OpenLDAP* bezbednosnim sistemima; **b)** koji tipovi podataka se čuvaju; **c)** kako su podaci povezani u informacionim bazama podataka; **d)** koje su sličnosti i razlike tipova podataka i njihovih atributa između dva različita sistema. U sledećem koraku su istražene sličnosti i razlike dva bezbednosna sistema, razvijen je interoperabilan adapter koji je funkcionalan sa oba sistema. Promenom konfiguracije na samo jednom mestu može da se pristupi drugom sistemu. Adapter sa *AD* – omi *OpenLDAP* – om je semantički interoperabilan, zato što su podaci koji se razmenjuju razumljivi i jednom i drugom sistemu.

## Funkcionalnosti

*AD* u svojoj bazi podataka čuva informacije o korisnicima, grupama, računarima, kompjuterima, štampačima, aplikacijama i servisima. Za razliku od *AD*, *OpenLDAP* u svojoj osnovnoj šemi čuva podatke samo o korisnicima i grupama, pa su se prilikom implementacije rešenja realizovale funkcije za rad samo sa tim entitetima. Iako se imena entiteta na dva različita sistema poklapaju, imena tipova atributa su različita. Zato je izvršeno mapiranje atributa entiteta sa generičkog sloja, sa semantički jednakim atributima entiteta sa *AD* – a i *OpenLDAP* – a. Mapiranje je prikazano na *Tabeli 1* i *Tabeli 2*. U *Tabeli 1* se vidi mapiranje atributa korisnika, a u *Tabeli 2* kako su mapirani atributi grupe.

|  |  |  |
| --- | --- | --- |
| *GenericUser* | *AD User* | *OpenLDAP User* |
| *username* | *userPrincipalName* | *cn* |
| *name* | *givenName* | *givenName* |
| *surname* | *surname* | *sn* |
| *password* | *password* | *userPassword* |
| *phoneNumber* | *voiceTelephoneNumber* | *mobile* |
| *emailAddress* | *emailAddress* | *mail* |
| *description* | *description* | *description* |
|  |  | *Distinguished-Name* |

*Tabela 1* - Mapiranje korisničkih atributa sa generičkog sloja na atribute na *AD* i *OpenLDAP* atribute korisnika

|  |  |  |
| --- | --- | --- |
| *Group* | *AD Group* | *OpenLdap Group* |
| *groupName* | *name* | *cn* |
| *Members<string>* | *Members<PrincipalCollection>* | *Members<string>* |
| *description* | *description* | *description* |
|  |  | *Distinguished-Name* |

*Tabela 2* - Mapiranje grupnih atributa sa generičkog sloja na atribute na *AD* i *OpenLDAP* atribute grupe

Za prikazane entitete razvijene su dve grupe funkcija: administratorske i korisničke. Administratorske funkcije (*Tabele 3, 4 i 5*) obuhvataju dodavanje, modifikovanje i brisanje iz baze podataka, a korisničke funkcije logovanje i proveru dozvole pristupa (*Tabela 6*).

|  |  |
| --- | --- |
| *CreateUser* | Kreiranje korisnika |
| *DeleteUser* | Brisanje korisnika |
| *ChangerUserUsername* | Izmena jedinstvenog imena korisnika |
| *ChangeUserName* | Izmena imena korisnika |
| *ChangeUserSurname* | Izmena prezimena korisnika |
| *ChangeUserPassword* | Izmena lozinke korisnika |
| *ChangeUserEmail* | Izmena adrese elektronske pošte korisnika |
| *ChangeUserPhoneNumber* | Izmena broja telefona korisnika |
| *ChangeUserDescription* | Izmena opisa korisnika |
| *CreateGroup* | Kreiranje grupe |
| *ChangeGroupName* | Izmena jedinstvenog imena grupe |
| *DeleteGroup* | Brisanje grupe |

*Tabela 3* – Administratorske funkcije za manipulisanje korisnicima i grupama

|  |  |  |
| --- | --- | --- |
| *AddUserToGroup* | | Dodavanje korisnika u grupu |
| *AddGroupToAnotherGroup* | Dodavanje grupe u drugu grupu | |
| *IsMemberOf* | Proveravanje članstva | |
| *GetAllGroupMembers* | Dobavljanje članova | |
| *CreateCustomPermission* | Kreiranje nove dozvole | |
| *AssignCustomPermission* | Dodeljivanje dozvole | |
| *ListAllUsers* | Izlistavanje korisnika | |
| *ListAllGroups* | Izlistavanje grupe | |

*Tabela 5 –* Administratorske funkcije

|  |  |
| --- | --- |
| *Login* | Logovanje |
| *CheckPermission* | Proveravanje dozvole |

*Tabela 6* – Korisničke funkcije

# Rezultati i analiza

## Testno okruženje

Za testno okruženje u ovom istraživanju instalirani su *Windows Server 2019* i *Linux* operativni sistem *Ubuntu 18.04.* Bezbednosni sistem ADje instaliran na *Windows Server* OS. Drugi sistem na kojem je testirano rešenje je *OpenLDAP,* verzija *2.4.48.*

Korišćene su i sledeće verzije programskih biblioteka:

* *Novell.Directory.Ldap 3.1.0*
* *System.DirectoryServices 4.6.0*
* *System.DirectoryServices.AccountManagement 4.6.0*

Za verifikaciju korišćena je procesna virtuelna mašina *Microsoft.NETCore.App 2.1*, na programskom jeziku *C#.*

## Testiranje

Za verifikaciju rešenja, razvijena je korisnička aplikacija koja nudi unos korisničkih i grupnih podataka za kreiranje novih entiteta, pretragu korisnika za modifikovanje i brisanje entiteta. Implementirana je i testirana mogućnost promene informaciono bezbednosnog sistema. Korinička plikacija poziva funkcije sa generičkog sloja i prikazuje stanje *AD* i *OpenLDAP* baze informacionih podataka.

Za verifikaciju generičkog sloja testni slučaj je obuhvatio:

1. Kreiranje pedeset novih korisnika i pet novih grupa
2. Učlanjenje korisnika u grupe
3. Izmena atributa kod korisnika i grupa
4. Logovanje korisnika
5. Kreiranje i dodeljivanje dozvola pristupa
6. Provera dozvole pristupa

Uspešno su testirane sve funkcionalnosti na oba bezbednosna sistema, a rezultat je verifikovan izlistavanjem svih korisnika i grupa, proverom članstva u grupama, a za funkcije logovanja korisnika su verifikovani fajlovi za praćenje logovanje korisnika.

# Zaključak

U današnje vreme bezbednost predstavlja jedan od najbitnijih faktora za uspešan rad softvera i poslovanje kompanija. U ovom radu istraženi su bezbednosni sistemi za upravljanje informacionim podacima o korisnicima, grupama i njihovim vezama. Za razumevanje motiva korišćenja informaciono bezbednosnih servisa, potrebno je bilo da se definišu sledeći koncepti bezbednosti: kontrola pristupa, osnovni pojmovi i uloga informaciono bezbednosnih servisa i korišćenih protokola. Za ovaj rad su izabrane dve različite implementacije prokola *LDAP*, *AD* zasnovan na *Windows* platformi i *OpenLDAP*, zasnovan na *Linux* platformi. Instraženi su interfejsi za pristupanje informacionim bazama podataka na oba sistema, dizajniran je i implementiran interoperabilan adapter koji je kompatibilan sa obe LDAP implementacije bezbednosnih sistema. Adapter se nalazi na generičkom sloju, funkcionalnom na oba *OS* – a. Kompanijama je omogućen izbor između platforme za rad sa informaciono bezbednosnim sistemima, ali i jednostavna promena platforme, sa kojom će funkcionalnosti za upravljanje informacionim podacima ostati nepromenjene.

Generički sloj se može proširiti i unaprediti na nekoliko načina. Jedno rešenje je da se omogući pristup još jednom informaciono bezbednosnom sistemu. Dodatni sistem bi proširio opseg mogućih korisnika i usluga ovog rešenja. Drugo rešenje je da se omogući proširenje postojeće šeme na *AD* – u i *OpenLDAP* – u, čime bi novi tipovi entitea kreirali u toku rada adaptera.

# Literatura

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security Fourth Edition*, no. January 2015. 2011.

[2] E. Harold F. Tripton, *Official (ISC) Guide To The SSCP CBK*. 1385.

[3] S. Tuttle *et al.*, “Understanding LDAP Design and Implementation,” pp. 1–774, 2006.

[4] B. Desmond, J. Richards, R. Allen, and A. Lowe-Norris, *Active Directory, 5th Edition*, vol. 91, no. 5. 2012.

[5] M. Butcher, *Mastering OpenLDAP - Configuring, Securing and Integrating Directory Services*. 2007.

[6] Techopedia, “Interoperability.” [Online]. Available:https://www.techopedia.com/definition/631/interoperability.

|  |  |
| --- | --- |
|  | **Kratka biografija**  Kandidat Aleksandar Maričić je rođen 30.5.1995. godine u Zrenjaninu. Završio je Gimnaziju u Zrenjaninu 2014. godine. Fakultet tehničih nauka u Novom Sadu je upisao 2014. godine, a Osnovne akademske studije završio je 2018. godine. Ispunio je sve obaveze i položio je sve ispite predviđene studijskim programom. |