UDC: 004.738.12.056.52 INFO M: str. 33-39

KONTEKSTNO ZAVISNA KONTROLA PRISTUPA
CONTEXT-SENSITIVE ACCESS CONTROL

Goran Sladić, Branko Milosavljević, Zora Konjović

REZIME: U današnjem dobu informacionih tehnologija kontrola pristupa, obično, razmatra na koji način korisnici mogu pristupati resursima računarskog sistema ili „ko šta može da radi“. Kontrola pristupa predstavlja, neosporivo, osnovni sigurnosni mehanizam koji je danas u upotrebi. Tradicionalni modeli kontrole pristupa, poput RBAC-a (Role Based Access Control), ne razmatraju uticaj kontekstualnih informacija prilikom definisanja i sprovođenja kontrole pristupa. Stoga, ovi modeli u određenim slučajevima korišćenja nisu adekvatni za definisanje i sprovođenje kontrole pristupa. Kontekstno zavisna kontrola pristupa eksplicitno razmatra kontekst (stanje okruženja) u specifikaciji i implementaciji mehanizama kontrole pristupa. Većina istraživanja u ovoj oblasti bazirana je na ekstenziji RBAC modela u cilju da podrži kontekstno zavisnu kontrolu pristupa. U radu je dat prikaz odabranih kontekstno zavisnih modela za kontrolu pristupa koji se primenjuju u različitim oblastima.
KLJUČNE REČI: kontrola pristupa, RBAC, kontekstno zavisna kontrola pristupa, kontekst, kontekstno zavisno računarstvo
ABSTRACT: In today’s information technology era, access control is concerned with the way in which users can access resources in a computer system, or informally speaking, with “who can do what”. Access control is arguably the most fundamental security mechanism in use today. Traditional access control models, such as RBAC (Role Based Access Control), are passive access control models. They do not take into account contextual information. Consequently, these models are inadequate for specifying access control needs of many complex real world cases. As context data gets involved, the access decision no longer depends on user credentials only, it also depends on the state of the system’s environment and the system itself. Most research in this area is based on extensions of the RBAC model to support context-sensitive access control. This paper gives overview of the selected context-sensitive access control models applied in different areas.
KEY WORDS: access control, RBAC, context-sensitive access control, context, context-sensitive computing

1. UVOD

Kontrola pristupa, odnosno autorizacija, u širem smislu, razmatra na koji način korisnici mogu pristupiti resursima računarskog sistema i na koji način ih koristiti.

Kontrola pristupa predstavlja samo jedan aspekt složene i obimne oblasti bezbednosti računarskih sistema, ali je i jedan od njenih najvažnijih delova. Ona učestvuje u obezbeđivanju poverljivosti i integriteta informacija. Poverljivost informacija podrazumeva da samo autorizovani korisnici mogu da pročitaju informacije, dok integritet informacija podrazumeva da samo autorizovani korisnici mogu da menjaju podatke u skladu sa sigurnosnom politikom posmatranog sistema.

Jedan od najčešće korišćenih modela za kontrolu pristupa u savremenim poslovnim sistema je model kontrole pristupa zasnovane na korisničkim ulogama (*Role Based Access Control*, RBAC) [14], gde je pristup objektima sistema baziran na ulozi korisnika u sistemu. Osnovni RBAC model čine sledeći entiteti: *korisnici*, *korisnička sesija*, *korisničke uloge* i *privilegije*, pri čemu se privilegije sastoje od *operacija* koje se izvršavaju nad *objektima*. Centralni deo RBAC-a predstavlja koncept uloge oko koje su formulisana prava pristupa. Osnovna relacija modela je povezivanje uloga i privilegija. U RBAC-u, ulogama se dodeljuju privilegije, a korisnicima se dodeljuju određene uloge. Prednost RBAC modela u odnosu na druge modele kontrole pristupa je u efikasnijem definisanju prava pristupa i administraciji sistema. RBAC entiteti obično se definišu na istom nivou apstrakcije kao i poslovni procesi organizacije za koju se RBAC model definiše. Osim osnovnog RBAC modela u literaturi, a i u praksi se susreću različite modifikacije i proširenja ovog modela. RBAC standardom pored osnovnog modela definisana su i njegova tri proširenja: hijerarhija uloga, statičko (*Static Separation of Duties*) i dinamičko (*Dynamic Separation of Duties*) razdvajanje obaveza, i kombinacija hijerarhije uloga sa razdvajanjem obaveza.

Glavna prednost u korišćenju ovog modela odgleda se u jednostavnoj administraciji prava pristupa i njegovoj skalabilnosti. Kada korisnik promeni radno mesto u organizaciji, administrator treba samo da korisniku dodeli neke nove uloge i ukloni mu stare.

Međutim, i dalje postoji značajan broj problema kada se, koristeći RBAC, opisuju neki složeni zahtevi kontrole pristupa. Tradicionalni modeli kontrole pristupa, poput RBAC-a, ne razmatraju uticaj kontekstualnih informacija (poput podataka koji se obrađuju, vremena, lokacije, itd.) prilikom definisanja i sprovođenja kontrole pristupa. Stoga, ovi modeli u određenim slučajevima korišćenja nisu adekvatni za definisanje i sprovođenje kontrole pristupa.

U slučajevima kada na kontrolu pristupa utiče kontekst dozvola pristupa za korisnika neće više zavisiti samo od dodeljenih mu uloga, odnosno privilegija već i od stanja samog sistema kao i od njegovog okruženja.

2. KONTEKST I KONTEKSTNO ZAVISNO RAČUNARSTVO

Kada čovek komunicira sa čovekom, oni su u stanju da u komunikaciji implicitno koriste informacije trenutne situacije (*konteksta*) u kome se komunikacija odvija kako bi ona imala potpuni smisao. Na žalost, ova mogućnost ne prenosi se direktno na komunikaciju čovek-računar. U tradicionalnim računarskim sistemima korisnici imaju relativno improvizovan mehanizam za prosleđivanje informacija korisniku. Obezbeđujući računaru

pristup kontekstu povećava se bogatstvo u načinu komunikacije čoveka i računara i pruža mogućnost da računar obezbeđuje korisnicima mnogo više korisnijih informacija [1].

U cilju efikasnog korišćenja konteksta potrebno je razumeti šta je kontekst, kako se može koristiti i potrebna je odgovarajuća arhitektura sistema. Razumevanje konteksta omogućuje dizajnerima aplikacije da odaberu koji kontekst da koriste u svojim aplikacijama. Razumevanje načina na koji se kontekst može iskoristiti omogućiće pravilan odabir kontekstno zavisnog ponašanja u aplikaciji. Na kraju, arhitektura jednog takvog sistema bi trebalo da obezbedi jednostavan i efikasan način njegove impelmentacije [10].

Kao tri osnovna aspekta konteksta autori u [32] navode: "*gde si*"' (*where are you*), "*s kim si*" (*who you are with*) i "*koji resursi su u blizini"* (*what resources are nearby*). Pod kontekstno zavisnim računarstvom podrazumeva se sistem sposoban da se adaptira lokaciji korišćenja, korisnicima koji ga koriste ili se nalaze u okruženju sistema, računarima i ostalim uređajima od kojih je sistem sačinjen, kao i da reaguje na promene ovih faktora.

U radovima [1, 10] date su najčešće korišćene definicije konteksta i kontekstno zavisnog računarstva:

Kontekst je bilo koja informacija koja se može koristiti za karakterizovanje situacije (stanja) entiteta. Entitet je osoba, mesto ili objekat koji se smatraju relevantnim za interakciju korisnika i aplikacije, uključujući samog korisnika i aplikaciju.

Sistem je kontekstno zavisan ako koristi kontekst da bi obezbedio relevantne informacije i/ili servise korisniku, gde relevantnost zavisi od korisnikovih zadataka.

U praksi postoji više različitih mehanizama za predstavljanje (modelovanje konteksta). U radovima [29, 30, 35] identifikovano je šest najčešće korišćenih pristupa:

- modelovanje posredstvom parova ključ-vrednost (*key-value*),
- modelovanje XML baziranim jezicima,
- modelovanje grafičkim jezicima (uglavnom UML),
- objektno orijentisano modelovanje,
- modelovanje logičkim jezicima, i
- modelovanje korišćenjem ontologija.

3. KONTEKSTNO ZAVISNA BEZBEDNOST

Kontekstno zavisna bezbednost eksplicitno razmatra kontekst u specifikaciji i implementaciji sigurnosnih mehanizama (kontroli pristupa, određivanju sigurnosnih nivoa, itd.) [5, 26, 27, 28]. Pojavom kontekstno zavisne bezbednosti pojavili su se i novi problemi sa stanovišta bezbednosti. Kako je kontekst uglavnom dinamičan, tj. često se menja, potrebno je obezbediti da se bezbednosni mehanizmi adaptiraju tim promenama, tj. da budu u stanju da efikasno reaguju na promene konteksta. U [27] data je definicija *sigurnosnog konteksta* kao:

Sigurnosni kontekst je skup informacija, sakupljenih iz okruženja korisnika i aplikacije, koje su relevantne sa stanovišta bezbednosne arhitekture za korisnika i/ili za aplikaciju.

4. RBAC BAZIRANI KONTEKSTNO ZAVISNI MODELI

U literaturi postoji veliki broj istraživanja na temu kontekstno zavisne kontrole pristupa. Uglavnom, u ovim istraživanjima nastoji se proširiti već postojeći modeli kontrole pristupa sa kontekstnim informacijama. Većina radova fokusirana je na ekstenziju RBAC modela kontrole pristupa. U ovom odeljku dat je pregled kontekstno zavisnih modela kontrole pristupa baziranih na RBAC-u.

4.1. *Opšti kontekstno zavisni RBAC bazirani modeli*

U radu [9] predstavljen je *Generalised Role-Based Access Control* (GRBAC) model kontrole pristupa. Ovaj model predstavlja ekstenziju RBAC modela koja omogućuje ne samo subjekat-orijentisan pogled na prava pristupa već i objekat-orijentisan i okruženje-orijentisan pogled, kao i kombinacije ova tri pogleda. GRBAC uklanja limitaciju RBAC modela (samo subjekat-orijentisan pogled) koristeći koncept uloge za organizovanje objekata nad kojim se sprovodi kontrola pristupa kao i za organizovanje okruženja u okviru koga se sprovodi kontrola pristupa. Po ovom modelu postoje tri tipa uloga: *uloge subjekta*, *uloge objekta* i *uloge okruženja*.

Uloge subjekta su analogne tradicionalnim RBAC ulogama. Jedina razlika između GRBAC-ovih uloga subjekta i tradicionalnih RBAC uloga je u načinu na koji se vrši provera prava pristupa. U tradicionalnom RBAC sistemu prava pristupa su u potpunosti bazirana na privilegijama dodeljenim ulogama koje subjekat poseduje. U GRBAC sistemu na pravo pristupa ne utiču samo uloge subjekta već i uloge objekta i uloge okruženja [9]. *Uloge objekta* omogućuju kreatoru prava pristupa da strukturira prava pristupa po obeležjima resursa sistema. Uloge objekta omogućuju da se po identifikovanju zajedničkih osobina nekih objekata oni grupišu u istu/iste uloge. Po grupisanju objekata moguće je vršiti kontrolu pristupa zavisnu od šeme grupisanja koja je korišćena. GRBAC omogućuje opisivanje stanja sistema posredstvom *uloga okruženja*. Uloge okruženja mogu da se baziraju na bilo kom stanju sistema koje može da se precizno evidentira. Aktivacija odnosno deaktivacija odgovarajuće uloge okruženja zavisi od stanja okruženja, tj. od odgovarajućih *uslova okruženja* koji utiču na aktivaciju/deaktivaciju određene uloge okruženja.

Da bi subjekat S pristupio objektu O, S mora da poseduje neku ulogu R_S tako da:

- postoji neka uloga objekta R_0 koju poseduje O,
- postoji neka uloga okruženja R_E koja je trenutno aktivna, i
- postoji neka neka privilegija P koja dozvoljava R_S da pristupi objektima u ulozi R_O kada je R_E aktivna.

U tradicionalnim sistemima za kontrolu pristupa zahtev mora da specificira ko želi da izvrši koju akciju nad kojim objektom. U kontekstno zavisnim sistemima za kontrolu pristupa pored ovih elemenata zahtev mora da obezbedi i odgovarajuće kontekstne informacije o subjektu, tj. zahtev je formalno definisan kao [20]:

$$Request = Subject \times Object \times Action \times SimpleContext$$

U prethodnoj definiciji *SimpleContext* je podskup konteksta *Context* jer nije moguće u zahtevu obezbediti sve informacije iz konteksta.

Kumar i dr. predložili su u članku [22] kontekstno zavisan RBAC model u kome su kontekstne informacije uvedene na

dva nivoa: na nivou korisnika (sadrži informacije o korisniku relevantne sa aspekta bebednosti) i na nivou objekta (sadrži informacije o objektu relevantne sa aspekta bezbednosti).

Strembeck i Neumann u članku [36] analiziraju kontekstno zavisno proširenje RBAC-a kroz različita ograničenja definisana RBAC modelom. Autori navode da pored klasifikacije na *statička* (npr. statičko razdvajanje obaveza) i *dinamička* (npr. dinamičko razdvajanje obaveza) ograničenja moguća je i klasifikacija na *endogena* (*interna*) i *egzogena* (*spoljašnja*). Pod endogenim ograničenjima podrazumevaju se ona ograničenja koja se odnose na entitete RBAC modela. Npr. endogeno ograničenje može biti statičko razdvajanje obaveza jer se ono odnosi na uloge koje su jedne od RBAC entiteta. Za razliku od endogenih, egzogena ograničenja odnose se na entitet koji nisu osnovni RBAC entiteti već su oni definisani kao sporadični uslovi izvesnih operacija sistema za kontrolu pristupa. Primer ovih ograničenja može biti vremensko ograničenje koje ograničava aktivaciju uloge za određeni vremenski period. Osim kategorizacije ograničenja na statička/dinamička i endogena/egzogena autori definišu podelu ograničenja i na *autorizaciona ograničenja* i *ograničenja dodele*. Autorizaciona ograničenja su ograničenja koja unose dodatnu logiku u procesu sprovođenja kontrole pristupa. Tako da, iako korisnik poseduje privilegije za izvršenje određene operacije, izvršenje će se odobriti isključivo ako su i odgovarajuća autorizaciona ograničenja zadovoljena. Npr. ovakva ograničenja mogu se primeniti da bi se implementirala kontrola pristupa zasnovana na istoriji pristupa. Ograničenja dodele su ograničenja kojima se kontroliše dodela privilegija ulogama (npr. maksimalni i minimalni kardinalitet, razdvajanje obaveza). Pojam *kontekstnog ograničenja* autori definišu kao uslove koje određeni atributi konteksta moraju da zadovolje da bi se odobrila zahtevana operacija. U odnosu na prethodno opisane kategorizacije kontekstna ograničenja su definisana kao dinamična egzogena autorizaciona ograničenja, a definisano je preko pojma kontekstnog atributa, kontekstne funkcije i kontekstnog uslova:

Kontekstni atribut predstavlja odgovarajuće obeležje okruženja čija aktuelna vrednost može dinamički da se menja. *Kontekstna funkcija* je mehanizam za preuzimanje tekuće vrednosti određenog kontestnog atributa. Kontekstna funkcija može da ima i svoje parametre. *Kontekstni uslov* je predikat (logička funkcija) koja se sastoji od operatora i dva ili više operanada. Prvi operand je uvek određeni kontekstni atribut, dok drugi operand može biti kontekstni atribut ili konstantna vrednost.

Kontekstno ograničenje je klauzula koja sadrži jedan ili više kontekstnih uslova. Ona je zadovoljena akko su svi kontekstni uslovi zadovoljeni. Kontekstna ograničenja se koriste za definisanje uslovnih privilegija. U skladu sa prethodno definisanim terminima, *uslovna privilegija* je privilegija kojoj je pridruženo jedan ili više kontekstnih ograničenja.

Bao i dr. predstavili su u [3] *Conditional RBAC* (C-RBAC) model kontrole pristupa. Ovaj model predstavlja proširenje RBAC modela uvođenjem *atributa uloge* i *konteksta* koji je opisan preko *kontekstnih atributa*. Osim ovih etiteta, C-RBAC uvodi i pojam *uslovne uloge* koja je definisana kao par (*uloga*, *uslovni_izraz*), gde *uslovni_izraz* predstavlja logički izraz koji se sastoji od atributa uloge, kontekstnih atributa i operatora $\{<, \leq, >, \geq, =, \neq, \wedge, \vee\}$. U C-RBAC-u pristup resursu je dozvoljen ako je za bilo koju uslovnu ulogu, uloge koja je dodeljena korisniku, dozvoljen pristup resursu i ako je zadovoljen uslov te uslovne uloge.

Predlog UML modela za kontekstno bazirani model za kontrolu pristupa dat je u [13]. Predloženi model identifikuje dva tipa konteksta (logički i fizički), korisnike, resurse, profile korisnika, uređaja kao i servisa (zadataka) koje dati sistem obezbeđuje. Korisnicima su prava pristupa odgovarajućim resursima dodeljena posredstvom konteksta, tj. dozvola pristupa korisnika odgovarajućem resursu zavisi od prava pristupa definisanih za aktivne kontekste.

4.2. *Kontekstno zavisni RBAC bazirani modeli u poslovnim sistemima*

U radovima [18, 34] predstavljen je model kontekstno zavisne kontrole pristupa za poslovne sisteme. Dati model je zasnovan na standardnom RBAC modelu kontrole pristup koji je proširen entitetima *poslovnog procesa*, *aktivnostima*, *kontekstom* i *kategorijama resursa*. Uvođenjem entiteta *poslovnog procesa* i *aktivnosti* omogućeno je efikasnije definisanje i sprovođenje kontrole pristupa za poslovne procese. S obzirom da je moguće da na kontrolu pristupa utiču i faktori iz okruženja samog sistema pa i faktori koji čine sam sistem ali ne i eksplicitno model kontrole pristupa, predloženi model proširen je i *kontekstom*. *Kategorizacija resursa* omogućuje definisanje prava pristupa za čitavu kategoriju (grupu) resursa i time potencijalno smanjuje broj prava pristupa koje je potrebno definisati.

Za modelovanje konteksta odabran je ontološki pristup, pri čemu je kontekst definisan koristeći OWL (Web Ontology Language) jezik. Ovaj model definiše tzv. *domensku ontologiju* (*domain ontology*) za kontekst u poslovnim sistemima (za potrebe kontrole prsitupa), kojim su modelovane bazične klase i obeležja konteksta. Za primenu u konkretnom okruženju predloženi ontološki model potrebno je proširiti uvođenjem specijalizacija datih entiteta, uvođenjem novih entiteta kao i novih relacija. Dati kontestni model definiše dve osnovne vrste koncepata (klasa): *kontektne činjenice* i *kontekstne izraze*. *Konteksnte činjenice* modeluju elementarne kontekstne informacije, dok *kontekstni izrazi* predstavljaju semantičko povezivanje ovih činjenica [18, 34].

Sekvencu događaja, *striktne najmanje privilegije* i *separaciju obaveza* autori u radu [7] svrstavaju među najznačajnije zahteve kontrole pristupa u *workflow* sistemima. Da bi se obezbedili navedeni zahtevi predložen je kontekstno zavisan RBAC model za *workflow* okruženja. Pod kontekstnim informacijama u ovom modelu se podrazumevaju definicije i instance procesa i zadataka (*task*-ova) kao i njihove međusobne relacije. Uloga kojoj je dozvoljeno da izvrši odgovarajući *task* identifikovana je relacijom između *task*-ova i uloga. Takođe, između *task*-ova uvedena je relacija kojom su definisani međusobno konfliktni *task*-ovi. Korisnik će posedovati različite privilegije zavisno od tekućeg *task*-a koga izvršava. Ove privilegije ne samo da se razlikuju sa vremenom, već su uvek apsolutni minimum privilegija potrebnih da se izvrši *task*.

Georgiadis i dr. predstavili su u [17] *Context based TMAC* (C-TMAC) model za kontrolu pristupa u kolaborativnim sistemima. Ovaj model predstavlja integraciju TMAC (*Team-based Access Control*) [37] i RBAC koncepata zajedno sa kontekstnim informacijama. Korisniku su pored uloga dodeljeni i timovi, pri čemu tim predstavlja grupu korisnika, sa specifičnim ulogama,

formiran u cilju završetka neke aktivnosti u određenom kontekstu. Međutim, koncept timova se koristi i kao mehanizam povezivanja korisnika i konteksta, ekvivalentno kao što se uloge koriste za povezivanje korisnika i privilegija.

X-GTRBAC okruženje [4] zasnovano je na GTRBAC (Generalized Temporal Role-based Access Control) modelu [23], tj. predstavlja implementaciju GTRBAC modela i namenjen je za sprovođenje kontrole pristupa u različitim poslovnim sistemima. Za predstavljanje entiteta definisanih GTRBAC modelom i njihovih međusobnih relacija iskorišćen je XML jezik. Osim za korišćenje u poslovnim sistemima, u radu [4] pokazano je na koji način bi se X-GTRBAC okruženje moglo primeniti u web servis baziranim sistemima. Za potrebe primene u ovakvim sistemima model X-GTRBAC je proširen da podržava i kontekstno zavisnu kontrolu pristupa zasnovanu na temporalnim kontekstnim uslovima, ali i na kontekstnim uslovima koji nisu temporalni. Formalni model konteksta definisan u X-GTRBAC-u bazira se na GTRBAC modelu, a zasnovan je na sledećim entitetima:

- *PN* - je skup svih mogućih naziva za kontekstne parametre,
- *RT* - je skup svih mogućih tipova kontekstnih parametara,
- *kontekstni parametar* definisan je kao struktura podataka *p* koja ima sledeća obeležja $p \in PN$, $type \in PT$ i funkciju *getValue*(),
- *skup uloga* - $RR = \{rr_1, rr_2, ..., rr_k\}$, gde je rr_i, $i = 1, ..., k$ regularna uloga u GTRBAC modelu,
- *skup operacija* - $RO = \{ro_1, ro_2, ..., ro_k\}$, gde je ro_i, $i = 1, ..., k$ regularna operacija u GTRBAC modelu, i
- *skup servisa* - $SRVS = \{srv_1, srv_2, ..., srv_k\}$, gde je srv_i, $i = 1, ..., k$ servis, gde se pod pojmom servisa podrazumeva apstrakcija operacija koju obezbeđuje sistem nad nekim svojim resursima. Formalno servis je podskup skupa operacija *RO*.

Na osnovu ovih entiteta definisani su sledeći pojmovi:

Kontekstni skup *C* sastoji se od *n* kontekstnih parametara $\{p_1, ..., p_n\}$, $n \geq 0$, pri čemu važi $p_i.name \neq p_j.name$ za svaki p_i, p_j gde je $i \neq j$, $1 \leq i, j \leq n$, tj. ne mogu da postoje dva parametra sa istim imenom.

Zahtev za izvršenje servisa definisan je kao trojka (*role, srv, contextset*) gde je $role \in RR$, $srv \in SRVS$, a *contextset* (kontekstni skup) je definisan u skladu sa prethodnom definicijom.

Na osnovu pristiglog zahteva za izvršenjem servisa sistem određuju se primenjiva prava pristupa za traženi servis. Ovaj postupak, pored navedene uloge i servisa zavisi i od ograničenja definisanih za navedenu ulogu kao i od definisanih kontekstualnih podataka. Za svaku ulogu moguće je definisati skup kontekstnih atributa kojima je definisan kontekstno zavisan uslov za tu ulogu. Vrednosti ovih atributa definiše administrator, a te vrednosti se porede sa vrednostima kontekstnih parametara navedenim u zahtevu u cilju određivanja primenljivih prava pristupa. Skup kontekstnih atributa uloge je u stvari podskup kontekstnog skupa *C*.

4.3. *Kontekstno zavisni RBAC bazirani modeli u web servis okruženjima*

Rad [38] razmatra problem kontrole pristupa u web servis baziranim sistemima sa stanovišta kvaliteta (pouzdanosti) identifikacionog mehanizma kao kontekstno zavisnog parametra. Autori su predložili model kontrole pristupa zasnovan na RBAC modelu gde je u hijerarhiju uloga uključen i mehanizam identifikacije kojeg korisnik koristi. U sistemima (aplikacijama) koji poseduju različite mehanizme za proveru identiteta korisnika prava pristupa mogu da zavise od korišćenog mehanizma identifikacije. Npr. ako je korisnik identifikovan preko privatnog ključa i sertifikata može da ima veće privilegije u odnosu na slučaj kada je identifikovan preko korisničkog imena i lozinke. Kako su u klasičnom RBAC modelu različiti nivoi privilegija korisnika agregirani posredstvom uloga, mehanizam identifikacije korisnika osim na njegove privilegije utiče i na uloge i njihovu hijerarhiju. Zavisno od korišćenog mehanizma autentifikacije korisniku će u okviru tekuće sesije biti dodeljen odgovarajući skup uloga.

Kontekstno zavisan, servis-orijentisan RBAC model (*Context-aware Service-oriented RBAC*, CSRBAC) za kontrolu pristupa web servisima opisan je u radu [12]. U predloženom CSRBAC modelu ulogama se dodeljuju privilegije za pristup odgovarajućim servisima, gde se pod servisom podrazumeva apstrakcija operacija koje sistem obezbeđuje nad objektima. Kontekst u CSRBAC modelu predstavlja skup, sa stanovišta bezbednosti relevantnih, informacija u sistemu, npr. vreme, lokacija, prethodna stanja, itd. Odgovarajuća uloga, koja je dodeljena korisniku, će biti aktivna u okviru sesije tog korisnika ako su ispunjeni svi kontekstni uslovi potrebni za aktivaciju te uloge (ako navedeni kontekstni parametri zadovoljavaju zahtevane vrednosti).

Habio i Fan u radu [19] analiziraju problem bezbednosti u web servis baziranim aplikacijama, osvrćući se na problem kontekstno zavisne kontrole pristupa. Rad prikazuje kontekstno zavisan RBAC model za kontrolu pristupa, namenjen prvenstveno za web servise (*Context-aware Role-based Access Control*, CGRBAC). Opisani model rešava problem kontrole pristupa za procese realizovane posredstvom kompozitnih (globalnih) web servisa. Pod kompozitnim (globalnim) web servisima podrazumevaju se web servisi realizovani od atomskih (lokalnih) web servisa i/ili drugih kompozitnih web servisa. Dok se za atomske web servise prava pristupa mogu specificirati direktno, za kompozitne to nije slučaj. Prava pristupa za kompozitne web servise zavise od njegovih atomskih web servisa kao i od samog kompozitnog web servisa. U datom modelu objekti i operacije su zamenjeni *servisima*. Servis predstavlja skup operacija koje se mogu izvršiti nad određenim objektom, tj. servis predstavlja apstrakciju operacija nad nekim objektom koje dati sistem obezbeđuje. Uloge u modelu su podeljene na globalne i lokalne uloge. Korisniku su dodeljene globalne uloge, a globalnim ulogama se dodeljuju privilegije za izvršenje odgovarajućih globalnih servisa. U slučaju da globalni servis poziva neki lokalni servis, potrebno je izvršiti mapiranje globalnih uloga korisnika na lokalne uloge korisnika pošto su globalne uloge poznate samo provajderu globalnog servisa, ali ne i provajderima lokalnih servisa. Stoga je RBAC model proširen i relacijom koja opisuje mapiranje globalnih uloga nekog provajdera na lokalne uloge drugih provajdera. Aktivacija globalnih uloga za korisnika zavisi od stanja okruženja, tj. od definisanih parametara okruženja, dok aktivacija lokalnih uloga zavisi od toga da li je pozvan lokalni servis za koga su te uloge definisane.

Problem kontrole pristupa u serivs-orijentisanim autonomnim decentralizovanim sistemima razmatran je u radu [39]. U

datom radu predložen je model i arhitektura sistema za kontrolu pristupa zavisnog od situacije (*Situation Aware Access Control*, SA-AC). Predloženi SA-AC model baziran je na RBAC modelu koji je proširen sa situacijski zavisnim ograničenjima (SA ograničenja) na dodelu uloga korisnicima i dodelu privilegija ulogama. Formalno, SA ograničenja su modelovana na sledeći način:

- U - je skup svih korisnika
- R - je skup svih uloga
- P- je skup svih privilegija
- $UR \subseteq U \times R$ - je skup svih korisnik-uloga dodela
- $RP \subseteq R \times P$ - je skup svih loga-privilegija dodela
- SE - je skup svih izraza kojima se opisuju situacije
- $SEUR \subseteq 2^{SE} \times UR$ - je skup situacijski zavisnih korisnik-uloga dodela. $seur = (L_{se}, (u, r))$, $seur \in SEUR$) definiše da ako su samo svi situacijski izrazi (situacije) u listi $L_{se} \subseteq SE$ zadovoljeni (tačni) tada je dodela $(u, r) \in UR$ aktivna
- $SERP \subseteq 2^{SE} \times RP$ - je skup situacijski zavisnih uloga-privilegija dodela; $serp = (L_{se}, (r, p))$, $serp \in SERP$) definiše da ako su samo svi situacijski izrazi (situacije) u listi $L_{se} \subseteq SE$ zadovoljeni (tačni) tada je dodela $(r, p) \in RP$ aktivna.

Kapasails i dr. u radu [21] predstavili su dinamičku, kontekstno zavisnu arhitekturu modula za kontrolu pristupa u web servis baziranim okruženjima. Mehanizam kontrole pristupa baziran je na RBAC modelu u koji su inkorporirane dinamičke kontekstne informacije u formi kontekstnih ograničenja.

Kontekst je definisan i kategorisan kao: *korisnički kontekst* koji predstavlja status korisnika koji pristupa resursu, *kontekst resursa* koga čini status resursa kome se pristupa, *kontekst okruženja* koji predstavlja status bilo kojih entiteta relevantnih za specifični zahtev i *istorijski kontekst* koji se sastoji od specifičnih, prethodno izvršenih događaja i situacija, koji konstituišu dodatnu dimenziju kontekstnih informacija uključujući istoriju vezanu za korisnike, resurse i okruženje.

RBAC model je proširen kontekstno zavisnom kontrolom pristupa tako da korisnik koji pripada određenoj ulozi ima određenu privilegiju dodeljenu toj ulozi samo ako i zadovoljava navedeno *kontekstno ograničenje*. Kontekstno ograničenje je definisano kroz pojmove *kontekstnih podataka*, *akvizicije kontekstnih podataka* i *kontekstnog uslova*, pri čemu kontekstni uslov može biti prost i složen. *Kontekstni podatak* predstavlja bilo koji podatak relevantan za entitete kontrole pristupa. *Akvizicija kontekstnih podataka* je u stvari mehanizam pomoću koga su kontekstni podaci sakupljeni. *Prosti kontekstni uslov* je predikat koji proverava validnost uslova i sastoji se od operatora i dva operanda. Prvi operand je uvek kontekstni podatak, dok drugi takođe može biti kontekstni podatak ili predefinisana vrednost. Prosti kontekstni uslov uvek vraća logičku vrednost (tačno ili netačno). *Kompozitni kontekstni uslov* se definiše kao logički izraz koji se sastoji od logičkih operatora i jednog ili više operanda, pri čemu operandi mogu biti prosti kontekstni uslovi ili drugi složeni kontekstni uslovi. Kontekstno ograničenje sastoji se od jednog ili više prostih i/ili složenih kontekstnih uslova.

Kontekstno zavisni dinamički RBAC bazirani model (*Context Based Dynamic RBAC*, CDACM) za kontrolu pristupa u web servis okruženjima opisan je u radu [33]. Kontekst je definisan kao skup atributa, kontekstni uslov kao logički izraz koji sadrži kontekstni atribut, a kontekstno ograničenja kao skup kontekstnih uslova. Osnovne karakteristike ovog modela su sledeće [33]:

- mogućnost formiranja hijerarhije privilegija (privilegija sadrži privilegije nižeg nivoa),
- kontrola pristupa se sprovodi na dva nivoa; nivou servisa i nivou atributa (parametara/povratne vrednost) servisa, i
- ulogama su dodeljeni odgovarajući konteksti, a kontekstima privilegije, tj. dodela privilegija ulogama je posredstvom odgovarajućeg konteksta (kontekstnog ograničenja).

OASIS (*Open Architecture fore Secure Interworking Services*) model [2] dizajniran je da obezbedi kontrolu pristupa servisima u otvorenim distribuiranim sistemima. Uloge u ovom sistemu formirane su na osnovu servisa. Naziv uloga predstavlja odgovarajuću poslovnu funkciju ili zvanje u organizaciji, dok uloga predstavlja naziv uloge pridružen određenom servisu, par (*naziv uloge*, *servis*), tj. uloge su specifične za odgovarajući servis, a naziv uloge je jedinstven na nivou određenog servisa. Aktivacija uloga kontrolisana je na osnovu odgovarajućih pravila definisanih za tu ulogu. Ovim pravilima su definisani uslovi koje korisnik treba da zadovolji kako bi mogao da aktivira ulogu. Takođe, u pravilima mogu da se navode i parametari okruženja (ograničenja okruženja) čime je praktično obezbeđena kontekstna zavisnost OASIS modela.

4.4. *Kontekstno zavisni RBAC bazirani modeli u heterogenim računarskim sistemima*

Ubiquitous Context-based Security Middleware (UbiCOSM) sistem za sprovođenje kontrole pristupa u heterogenim mobilnim računarskim okruženjima opisan je radu [8]. Za razliku od klasičnog RBAC pristupa gde uloge predstavljaju posrednika između korisnika i privilegija, u UbiCOSM sistemu indirektna relacija između korisnika i privilegija ostvarena je posredstvom konteksta. Za svaki kontekst definiše se skup privilegija koji mu je pridružen. Kada se subjekat nalazi unutar odgovarajućeg konteksta, za njega se automatski aktivira skup privilegija koje su aktivne za navedeni kontekst. Prilikom promene konteksta privilegije prethodnog konteksta se uklanjaju, dok se privilegije novog konteksta dodeljuju subjektu. Opisani sistem razlikuje dva različita tipa konteksta: *fizički* i *logički*.

Fizički kontekst identifikuje fizički prostor, ograničen određenim geografskim koordinatama. U bilo kom vremenskom trenutku korisnik može da pripada (da se nalazi u) samo jednom fizičkom kontekstu. Logički kontekst identifikuje logičko stanje fizičkih konteksta ali i ostalih entiteta koje čine dati sistem (npr. korisnici, servis, itd.) Za razliku od fizičkog konteksta, korisnik u jednom vremenskom trenutku može pripadati većem broju logičkih konteksta. UbiCOSM posmatra identitet korisnika i korisničke uloge kao specifične tipove logičkog konteksta što omogućuje da se sistem koristi i kao subjekat-baziran sistem za kontrolu pristupa (npr. kao RBAC sistem).

Prava pristupa su definisana kao torka (*association_name*(*context_collection*), *permissions*). Prvi argument identifikuje kolekciju jednog ili više konteksta (*context_collection*) kojima će biti dodeljene privilegije (*permissions*). Sa *association_name* se definiše na koji način se ostvaruje veza između konteksta i privilegija. Moguće vrednosti za *association_name* su: *simple*, *and*, *or* i *dependence*. Vrednost *simple* omogućuje

dodeljivanje privilegija individualnom kontekstu, dok se ostale vrednosti primenjuju na kolekciju od više konteksta. U slučaju *and* asocijacije privilegije su aktivivirane ako su svi navedeni konteksti aktivni u isto vreme, dok će u slučaju *or* asocijacije privilegije biti primenjene ako je bar jedan od navedenih konteksta aktivan. Asocijacija *dependence* omogućuje izražavanje složenijih situacija koje mogu da se pojave. U osnovi ona omogućuje da se nekom mobilnom klijentu u okviru nekog konteksta dozvoli odgovarajuća akcija samo ako je u okviru istog fizičkog konteksta prisutan i neki drugi mobilni klijent. U slučaju ove asocijacije privilegije će biti primenjene kada je logički kontekst za datog mobilnog klijenta aktivan i kada su logički konteksti (koji su navedeni u relaciji) ostalih mobilnih klijenata (u istom fizičkom kontekstu) aktivni.

Liscano i Wang predstavili su u [25] mehanizam nadogradnje dRBAC [16] modela kontrole pristupa da podrži kontekstno zavisnu delegaciju za potrebe distribuiranih heterogenih računarskih sistema. Pod delegacijom se podrazumeva mogućnost da korisnik delegira neke svoje privilegije odnosno uloge nekom drugom korisniku. Kontekstualno proširenje dRBAC modela zasnovano je na modelu ontologija preuzetim iz [24], gde su kontekstualne informacije klasifikovane u *entitete* i *aktivnosti*. Entiteti su osobe, lokacije, vreme i resursi, a aktivnosti su ponašanja entiteta. Da bi se izbegla potreba za korišćenjem zajedničke kontekstualne ontologije između različitih strana, kontekstnualna ograničenja se primenjuju samo na stranu (organizaciju) koja je vlasnik resursa.

U radu [11] predložen je model kontekstno zavisne kontrole pristupa za heterogena mobilna računarska okruženja (*pervasive computing*). Po autorima većina sistema za kontrolu pristupa u ovoj oblasti zasnovana je na RBAC modelu koji je proširen tako što je omogućena kontekstno zavisna dodela privilegija ulogama, međutim dodela uloga korisnicima nije zavisna od konteksta što potencijalno može da izazove otežanu administraciju takvog sistema. Predloženi model zasnovan je na RBAC modelu koji je modifikovan kako bi bio efikasniji za heterogena računarska okruženja. Korisničke uloge su dinamički dodeljene korisnicima na osnovu dugotrajnih kontekstnih informacija, dok je dodela privilegija ulogama zavisna od kratkotrajnih informacija iz okruženja. Pod dugotrajnim kontekstnim informacijama podrazumevaju se informacije koje se ne menjaju unutar nekog vremenskog perioda Δt (npr. vremena trajanja sesije korisnika) dok se pod kratkotrajnim kontekstnim informacijama podrazumevaju informacije koje se unutar tog istog vremenskog perioda Δt mogu promeniti. Na početku sesije korisnicima su dodeljene određene uloge na osnovu definisanih informacija iz okruženja. Da bi se omogućila dinamička autorizacija aktivne privilegije dodeljene ulogama korisnika mogu da se menjaju za svakog korisnika ponaosob promenom okruženja.

Pigeot i dr. uočili su da je kontekstno zavisna kontrola pristupa u *pervasive computing* okruženjima često kompleksna i retko kad korisnički-orijentisana (komplikovana za definisanje). Zbog toga, predložen je gramatika jezika koja omogućuje korisnicima da na relativno jednostavan i efiksan način definišu kontekstno zavisna pravila, na osnovu njihove percepcije konteksta, koja će uticati na kontrolu pristupa [31].

Filho i Martin u radu [15] razmatraju primenu i uticaj *kvaliteta kontektne informacije* (*Quality of Context Information*), QoC) na kontekstno zavisnu kontrolu pristupa u *pervasive* računarskim okruženjima. Pod kvalitetom kontekstne informacije autori podrazumevaju definiciju datu u [6]: "*bilo koja informacija koja opisuje kvalitet informacije koja se koristi kao kontekstna informacij*" (npr. tačnost, preciznost, kompletnost, pouzdanost). Takođe, autori su dali i predlog merenja QoC informacija.

5. ZAKLJUČAK

Sa razvojem i primenom informacionih tehnologija u različitim oblastima problem efikasne bezbednosti dolazi do izražaja. Jedan od ključnih izazova u bezbednosti informacionih sistema je dizajn efikasnog mehanizma kontrole pristupa koji će adekavatno zadovoljiti sve zahteve kontrole pristupa. Da bi zadovoljili ove zahteve modeli kontrole pristupa treba da zavise i od kontekstnih informacija relevantnih sa stanovišta bezbednosti. Kontekstno zavisan model kontrole pristupa je u stanju da detektuje i reaguje na dinamičke promene u sistemu i okruženju samog sistema.

Tip kontekstnih informacija koje će se koristiti za potrebe kontrole pristupa zavisi od slučaja do slučaja. Moguće je da se koriste informacije poput vremena, lokacije, uređaja sa koga se pristupa, računarske mreže, itd. Naprednije solucije koriste i neke druge informacije iz samog sistema, ali i iz njegovog okruženja, kao i kombinovanje ovih osnovnih informacija u cilju izvođenja nekih novih.

RBAC model kontrole pristupa je danas jedan od najrasprostranjenijih modela za kontrolu pristupa sa primenom u različitim oblastima. Zbog svojih dobrih osobina RBAC model se vrlo često koristi kao osnova za razvoj kontekstno zavisnih modela kontrole pristupa, pri čemu se standardni RBAC model proširuje segmentima koji obezbeđuju kontekstno zavisnu kontrolu pristupa.

LITERATURA

[1] Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., Steggles, P. Towards a better understanding of context and contextawareness. In *HUC '99: Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, pp. 304–307, 1999.

[2] Bacon, J., Moody, K., Yao, W. A model of OASIS role-based access control and its support for active security. *ACM Transactions on Information and System Security*, 5(4):492–540, 2002.

[3] Bao, Y., Song, J., Wang, D., Shen, D., Yu, G. A role and context based access control model with UML. In *International Conference for Young Computer Scientists*, pp. 1175–1180, 2008.

[4] Bhatti, R., Ghafoor, A., Bertino, E., Joshi, J. X-GTRBAC: an XML-based policy specification framework and architecture for enterprisewide access control. *ACM Transactions* on Information and *System Security*, 8(2):187–227, 2005.

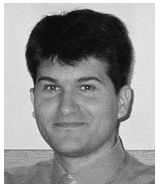
[5] Brezillon, P., Kouadri Mostefaoui, G. Context-based security policies: a new modeling approach. In *PERCOMW '04: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, p. 154, 2004.

[6] Buchholz, T., Kupper, A., Schiffers, M. Quality of context: what it is and why we need it. In *Proceedings of the Workshop of the HP Open View University Association (HPOVUA 2003)*, 2003.

[7] Cholewka, D., Botha, R., Eloff, J. A contextsensitive access control model and prototype implementation. In *Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures*, pp. 341–350, 2000.

[8] Corradi, A., Montanari, R., Tibaldi, D. Context-based access control for ubiquitous service provisioning. *Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC)*, pp. 444–451, 2004.
[9] Covington, M., Long, W., Srinivasan, S., Dev, A., hamad, M., Abowd, G. Securing context-aware applications using environment roles. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pp. 10–20, 2001.
[10] Dey, A. K. *Providing architectural support for building context-aware applications*. PhD thesis, Georgia Institute of Technology, Georgia, USA, 2000.
[11] Emami, S., Amini, M., Zokaei, S. A context-aware access control model for pervasive computing environments. *Proceedings of the IEEE International Conference on Intelligent Pervasive Computing (IPC)*, pp. 51–56, 2007.
[12] Feng, X., Jun, X., Hao, H., Li, X. Context-aware role-based access control model for web services. *Grid and Cooperative Computing - GCC2004 Workshops, International Workshop on Information Security and Survivability for Grid*, pp. 430–436, 2004.
[13] Fernandez, E., Larrondo-Petrie, M., Escobar, A. Contexts and context-based access control. *Proceedings of the 3rd International Conference on Wireless and Mobile Communications (ICWMC)*, pp. 73–78, 2007.
[14] Ferraiolo, D., Kuhn, R., Chandramouli, R. *Rolebased access control*. Artech Hous, 2003.
[15] Filho, J. B., Martin, H. Using context quality indicators for improving context-based access control in pervasive environments. In *EUC '08:Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 285–290, 2008.
[16] Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V. dRBAC: distributed role-based access control for dynamic coalition environments. In *International Conference on Distributed Computing Systems*, volume p. 411, 2002.
[17] Georgiadis, C., Mavridis, I., Pangalos, G., Thomas, R. Flexible team-based access control using contexts. In *SACMAT '01:Proceedings of the sixth ACM symposium on Access control models and technologies*, pp. 21–27, 2001.
[18] Gostojić, S., Sladić, G., Milosavljević, B., Konjović, Z. Context-sensitive Access Control Model for Government Services. *Journal of Organizational Computing and Electronic Commerce*. 2012, ISSN: 1091-9392. (in print)
[19] Haibo, S., Fan, H. A context-aware role-based access control model for web services. *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE)*, pp. 220-223, 2005.
[20] Han, W., Zhang, J., Yao, X. Context-sensitive access control model and implementation. *Proceedings of the 5th International Conference on Computer and Information Technology (CIT)*, pp. 757–763, 2005.
[21] Kapsalisa, V., Hadellisb, L., Karelisb, D., Koubiasc, S.A dynamic context-aware access control architecture for e-services. *Computers & Security*, 25(7):507–521, 2006.
[22] Kumar, A., Karnik, N., Chafle, G. Context sensitivity in role-based access control. *SIGOPS Oper. Syst. Rev.*, 36(3):53–66, 2002.
[23] Latif, U., Joshi, J., Bertino, E., Ghafoor, A. A generalized temporal role-based access control model. *IEEE Transactions on Knowedge. and Data Engineering*, 17(1):4–23, 2005.
[24] Li, Y., Hong, J., Landay, J. ContextMap: modeling scenes of the real world for context-aware computing. In *5th Int. Conf. on Ubiquitous Computing (Ubi-Comp2003)*, 2003.
[25] Liscano, R., Wang, K. A context-based delegation access control model for pervasive computing. In *AINAW '07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, pp. 44–51, 2007.
[26] Mostefaoui, K. G. Security in pervasive environments, what's next? In *In the proceedings of the 2003 International Conference on Security and Management(SAM'03)*, pp. 93–96, 2003.
[27] Ghita Kouadri Mostefaoui, K. G., Brezillon, P. A generic framework for contextbased distributed authorizations. In *In 4th International and Interdisciplinary Conference on Modeling and Using Context (Context'03)*, pp. 204–217, 2003.
[28] Mostefaoui, K. G., Brezillon, P. Modeling context-based security policies with contextual graphs. In *PERCOMW '04: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, p. 28, 2004.
[29] Najar, S., Saidani, o., Kirsch-Pinheiro, M., Souveyet, C., Nurcan, S. Semantic representation of context models: a framework for analyzing and understanding. In *CIAO '09: Proceedings of the 1st Workshop on Context, Information and Ontologies*, pp. 1–10, 2009.
[30] Park, M., Gu, M. S., Ryu, K. H. Context information model using ontologies and rules based on spatial object. In *Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques*, pp. 107–114, 2007.
[31] Pigeot, C. E., Gripay, Y., Scuturici, M., Pierson, J. M. Context-sensitive security framework for pervasive environments. In *ECUMN'07: Proceedings of the Fourth European Conference on Universal Multiservice Networks*, pp. 391–400, 2007.
[32] Schilit, B., Adams, N., Want, R. Context-aware computing applications. In *Proc of IEEE Workshop on Mobile Computing Systems and Applications*, pp. 85–91, 1994.
[33] Shang, C., Yang, Z., Liu, Q., Zhao, C. A context based dynamic access control model for web service. In *International Conference on Embedded and Ubiquitous Computing, IEEE/IFIP*, pp. 339–343, 2008.
[34] Sladić, G. *Model kontekstno zavisne kontrole pristupa u poslovnim sistemima*. doktorska disertacija, Fakultet tehničkih nauka, Novi Sad, 2012.
[35] Strang, T., Linnhoff-Popien, C. A context modeling survey. In *Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing,* 2004.
[36] Strembeck, M., Neumann, G. An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Transactions* on Information and *System Security*, 7(3):392–427, 2004.
[37] Thomas, R. Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. In *RBAC '97:Proceedings of the second ACM workshop on Role-based access control*, pp. 13–19, 997.
[38] Wolf, R., Keinz, T., Schneider, M. A model for contextdependent access control for web-based services with role-based approach. *Proceedings of the 14th IEEE International Workshop on Database and Expert Systems Applications (DEXA)*, pp. 209–214, 2003.
[39] Yau, S. S., Yao, Y., Banga, V. Situation-aware access control for serviceoriented autonomous decentralized systems. In *Proceedings otf the Autonomous Decentralized Systems,* pp. 17–24, 2005.

dr Goran Sladić, Fakultet tehničkih nauka, Univerzitet u Novom Sadu.
Kontakt: sladicg@uns.ac.rs
Oblasti interesovanja: bezbednost informacija, upravljanje dokumentima, workflow sistemi, XML tehnologije



prof. dr Branko Milosavljević, Fakultet tehničkih nauka, Univerzitet u Novom Sadu.
Kontakt: mbranko@uns.ac.rs
Oblasti interesovanja: pretraživanje informacija, upravljanje dokumentima, kontrola pristupa, digitalne biblioteke

prof. dr Zora Konjović, Fakultet tehničkih nauka, Univerzitet u Novom Sadu.
Kontakt: ftn_zora@uns.ac.rs
Oblasti interesovanja: veštačka inteligencija, upravljanje dokumentima, digitalne biblioteke, geoinformacioni sistemi