UDC: 004.021 Info M: str. 17-23

KOMPARACIJA MODELA ZAŠTITE INFORMACIJA
COMPARISON OF INFORMATION SECURITY MODELS

Dragan Korać
University of Belgrade, korac@teol.net

REZIME: Trend ubrzanog razvoja digitalnih tehnologija stvorio je potrebu povećanog širenja informacija među različitim organizacijama, institucijama, korporacijama, i sl. U tom pogledu kritično je da se osigura adekvatna zaštita informacija. Danas postoje brojni modeli zaštite koji se bave različitim aspektima zaštite informacija. U ovom radu daje se sveobuhvatni komparativni pregled osnovnih modela zaštite informacija kao što su Bell-LaPadula, Biba, Take-Grant, Sea-View i Clark Wilson. U tom komparativnom pregledu, Biba model je korišćen kao bazični model za komparaciju. Za razliku od drugih radova, ovi modeli su partikularno tretirani. Njihove prednosti i nedostaci su naglašeni u detalje. Na osnovu izvršene komparativne analize bazičnih modela nekoliko važnih izazova je identifikovano. Jedan od njih je da ne postoji savršen model zaštite tj. model koji pokriva sve bazične aspekte zaštite. Takođe, u ovom radu daje se kratki pregled bazičnih principa zaštite informacija. Na kraju, u ovom radu je diskutovano o problemima koji se pojavljuju u modelima zaštite, kao i prijedlozima za njihovo ublažavanje ili prevazilaženje.

KLJUČNE REČI: model, zaštita, informacija, Biba model.

ABSTRACT: The trend of rapid development of digital technologies is creating the need for increased sharing of information among various organizations, institutions, corporations, etc. In that regard, it is critically to ensure adequate information security. Nowdays, there is a number of the security models that address diferrent aspects of information security. In this paper, a comprehensive overview and comparison of basic models of information security such as Bell-LaPadula, Biba, Take-Grant, Sea-View i Clark Wilson is given. Biba model is used as the basic model for comparison. Unlike other papers, these models are particularly treated. Their advantages and disadvantages are emphasised in detail. Several important challenges are identified on the basis of performed comparative analysis of basic models. One of these is that there is no perfect security model i.e., model that it covers all basic security aspects. Also, in this paper a brief review of basic principles of information security is given. Finally, in this paper a discussion of problems that appear in security models is shown, as well as proposals for their mitigating or overcoming.

KEY WORDS: model, security, information, Biba model.

1. UVOD

Eksponencijalnim razvojem savremenih informatičkih tehnologija bliska budućnost je mnogo brže postala realnost. U tom kontekstu posmatranja pojam zaštite informacija se izdiferencirao kao najvažnije i najdelikatnije globalno strategijsko pitanje sa kojim se susreću sva društva i svi informacioni sistemi. Danas je gotovo nemoguće zamisliti neku oblast e-komunikacije (poslovne i društvene) bez njihove primjene. Stoga, pojam zaštite informacija je segmenat kojem se treba posvetiti pažnja, posebno kada se radi o informacija u kojima je pitanje zaštite od prvorazredne važnosti. Ubrzani razvoj tehnoloških i bežičnih mreža uslovio je povećanje novih i još organizovanih oblika prijetnji po informacionu sigurnost. Sa uporednim razvojem novih tehnologija nameće se potreba za učestalim preispitivanjem zaštite koja treba da ide u korak sa tehnološkim razvojem kako bi bila dovoljno upotrebljiva. Danas postoje brojni različiti modeli za zaštitu informacija. Modeli zaštite definišu osnovu za stvaranje politike zaštite [1]. Cilj svih modela zaštite je da definišu autorizovano i neautorizovano stanje sistema da ograniči kretanje sistema prema neautorizovanom stanju. Modeli su razvijeni prema tipu sistema za koji treba da budu korišćeni. Neki modeli su razvijeni da obezbijede zaštitu za operativni sistem dok drugi su razvijeni za specifične aplikacije kao što su baze podataka. Dakle, mnogi izazovi u modelima zaštite informacija zahtijevaju sveobuhvatan pristup i tehnike u postizanju što boljeg modela zaštite. Danas postoji mnoštvo razvijenih modela zaštite i teorija koji su korišćeni u zaštiti *e-government* prema tehničkim i ne-tehničkim pitanjima [2]. Međutim, modeli poput Bell-LaPadula [3], Biba [4], Clark Wilson [5], Take Grant [6] Sea-View [7] predstavljaju osnovne i najvažnije modele zaštite informacija. Njihov poseban značaj i važnost leži u činjenici što ovi modeli predstavljaju bazičnu osnovu za razvijanje svih drugih modela.

Potreba za zaštitom informacija posmatra se u dva ključna aspekta, vrijednosti pružene zaštite i ublažavanje zaštite na rizik. Takođe, neophodno je istaći da potreba za zaštitom informacija se ogleda i u pogledu značaja zaštite kompanijskog brenda i ugleda. Radi prevlasti na tržištu danas brojne suprostavljene kompanije ciljano ili slučajno, direktno ugrožavaju konkurentske informacije u vidu neovlašćenog otkrivanja, korumpiranja ili sprečavanja pristupa odbijanjem usluge – DoS/DDoS (*engl. denial of service/distribution denial of service*) i sl. Kompanije čine sve moguće kako bi zaštitile pristup osjetljivim informacijama, a time na najdirektniji način štite moć i snagu koju posjeduju. Efektivna zaštita informacija je implementirana, razumljiva, i odmjerena programskom politikom, procedurama i kontrolama koje konzistentno postižu saglasnost, kontrolu i zakonitost. Potreba za zaštitom informacija kao najvrijednijeg organizacionog resursa sadržani su u principima informacione zaštite.

Doprinos ovog rada: ovaj rad u odnosu na prethodne radove daje integrisani pregled i komparaciju bazičnih modela zaštite informacija kao što su *Bell-LaPadula, Biba, Take-Grant, Sea-View i Clark Wilson* model. U tom komparativnom pristupu

Biba model je zbog svoje jednostavnosti, lake primjenjivosti i integracionih povoljnosti korišćen kao model za poređenje. Takođe, u ovom radu dat je kratki pregled osnovnih principa informacione zaštite. Pored bazične zaštite informacija dat je pregled i dopunske zaštite informacija. Identifikovani su novi stari izazovi u pogledu razvoja modela zaštite koji treba da objedini sve bazične aspekte zaštite. Na kraju, ovaj rad diskutuje o problemima koji su prisutni u modelima zaštite i daje prijedloge za njihovo prevazilaženje ili ublažavanje.

Kratki pregled ovog rada je sljedeći: sekcija dva opisuje prethodne radove, dok sekcija tri daje kratki pregled osnovnih principa informacione zaštite. U sekciji 4 se daje opis osnovnih modela zaštite i njihovo poređenje sa Biba modelom. Sekcija pet diskutuje o problemima koji se pojavljuju u modelima zaštite. Sekcija šest daje zaključke.

2. PRETHODNI RADOVI

U dostupnoj literaturi, postoji mnogo radova koji se bave sa modelima zaštite, a čiji pristup je baziran na nekom od bazičnih aspekata zaštite. Primjeri su radovi poput [3] u kome su autori *Bell-LaPadula* primarni fokus usmjerili na povjerljivost kao bazični aspekt zaštite, dok je Biba u radu [4] fokus usmjerio na integritet kao bazični aspekt zaštite. Takođe, u modelu *Clark – Wilson* fokus je usmjeren na pitanje integriteta s tim što ovaj model predstavlja prošireno područje održavanja integriteta [5]. Postoje autori poput Denning et al. [7] koji su u svojim radovima istovremeno integrisali dva bazična aspekta zaštite. Oni su razvili *Sea – View* model koji pokriva tajnost i integritet. Autori poput Lipton et al. [6] razvili su *Take – Grant* model koji pokriva tajnost i povjerljivost. Model zaštite *Chinese Wall* je model koji podržava privatnost i integritet [8]. U radu Lipner [9] je razvio model koje se bavi pitanjima povjerljivosti i integriteta.

Dakle, razvoj većine modela zaštite bio je baziran na komparativnim sličnostima i različitostima između različitih modela. U dostupnoj literaturi, postoji mnogo radova koji su dali komparativni pregled osnovnih modela zaštite. Na primjer, Balon et al. [1] bavili su se poređenjem Biba modela sa *Take – Grant* i *Sea – View* modelom. Takođe, u radu Alharby [2] daje pregled najvažnijih modela zaštite i bavi se sa ne tehničkim modelima i teorijama. U radu [10], Anderson et al. bave se komparativnim pristupom između *Biba* i *Clark – Wilsona* modela. U radu [11], Clark et al. bave se komparacijom komercijalnih i politika kompjuterskih zaštita. U svim tim komparativnim metodama primjetno je da je *Biba* model korišćen kao model zaštite za poređenje. U ovom radu daje se sveobuhvatni pregled osnovnih modela zaštite u poređenju prema Biba modelu koji su kod drugih autora bili parcijalno tretirani. U cilju potpunijeg razumijevanja modela zaštite dat je kratki pregled osnovnih principa informacione zaštite.

3. PRINCIPI INFORMACIONE ZAŠTITE

Principi informacione zaštite su nasljeđeni elementi u politici zaštite i razvojnim rješenjima koji definišu osnovne parametre potrebne za zaštitno okruženje. Glavni cilj i svrha informacione zaštite sadržani su unutar bazične zaštite trojstva, a to su:

– Povjerljivost *(engl.Confidentiality),*
– Integritet *(engl. Integrity),*
– Raspoloživost *(engl. Availability)* – CIA[1], slika 1.

Slika 1. *Informaciono trojstvo*

Akronim CIA naziv je nastao od engleskih početnih slova zaštite trojstva tj. od tri osnovna zaštitna informaciona principa povjerljivost *(engl. confidentiality)*, integritet *(engl. integrity)* i raspoloživost *(engl. availability)*. Pored bazične zaštite informacija postoji i dopunska zaštita informacija:

– identifikacija (*engl. identification*),
– autentifikacije (*engl. authentication*),
– autorizacija (*engl. authorization*),
– provjera ili revizija (*engl. auditing*),
– tajnosti (*engl. secrecy*), i
– nemogućnosti poricanja informacija (*engl. non-repudiation*).

Sva tri bazična navedena principa čine jezgro načela informacione zaštite. U menadžmentu identiteta svaka aktivnost se oslanja na jedan od tri navedena principa informacione zaštite. Bitno je napomenuti, da principi informacione zaštite nisu uvijek svi podjednako zastupljeni. Najočitiji praktični primjer zastupljenosti sva tri principa informacione zaštite je u obavještajnim i policijskim agencijama te u vojnim institucijama.

4. OSNOVNI MODELI ZAŠTITE

4.1. *Model Bell-LaPadula (BLP)*

Model Bell-LaPadula (BLP) je razvijen od Bell i LaPadula (BLP) kao jedan od najranijih i najpoznatijih modela [3]. Ovaj model obezbijeđuje okvir za upravljanje klasifikovanim podacima i radi tog je nazvan višestruki model zaštite [12]. Svrha BLP modela je da dobije minimalne zahtijeve u pogledu

[1] Drugim permutacijama koncepta kao što su AIC su ponekad korišćeni da bi se izbjegla konfuzija sa najpoznatijom planetarnom obavještajnom agencijom.

povjerljivosti koji treba da budu zadovoljeni od strane bilo kog višestrukog sistema zaštite. Spada u jedan od najpopularnih modela zaštite koji štiti povjerljivost informacija unutar sistema. Postoje četiri komponente za BLP model [13]:

1. Subjekat su korisnici i sistem sposobni da izvrše procese,
2. Objekat su podaci elementa,
3. Čvorovi pristupa uključuju čitanje, pisanje, izvršavanje i mogućnost njihovog kombinovanja.
4. Zaštitni nivoi su suštitnski nivoi zaštitne klasifikacije.

BLP model se sastoji od sledeća dva stanja [14]:

1. Uslov jednostavne zaštite: subjekat ne može čitati podatke ako i samo ako nivo objekta je viši od nivoa subjekta, "*ne čitaj gore*".
2. Zvjezdano svojstvo: subjekat ne može pisati podatke ako i samo ako nivo subjekta je viši od nivoa objekta, "*ne piši dole*".

Ovaj model je zasnovana na informacionom toku u rešetci zaštitnih klasa, sa dopuštenim informacionim tokom samo u jednom pravcu rešetke. Informacioni tok BLP modela je zasnovan na *High Water Mark* principu, koji dopušta informacioni tok na-gore. Dakle, u ovom modelu dopušta se upotreba matričnog kontrolnog pristupa i zaštitnih nivoa pri čemu mandatorna pristupna kontrola sprečava informacioni tok samo između zaštitnih klasa. Politika zaštite zasnovana je na zaštiti informacija slijedeći od višeg nivoa prema nižem nivou. Kao što se može uočiti, glavni nedostatak ovog modela je da model ne riješava druga pitanja zaštite koja su definisana u jezgru informacione zaštite kao što je integritet i raspoloživost. Nažalost, mandatorne kontrole djelimično rješavaju probleme po pitanju trojanaca. Ipak, ovaj model i pored navedenih nedostataka još uvijek je korišćen kao višestruki model zaštite, posebno u vojne i obavještajne svrhe u kojima je povjerljivost podataka od prvorazredne važnosti.

4.2. *Biba model*

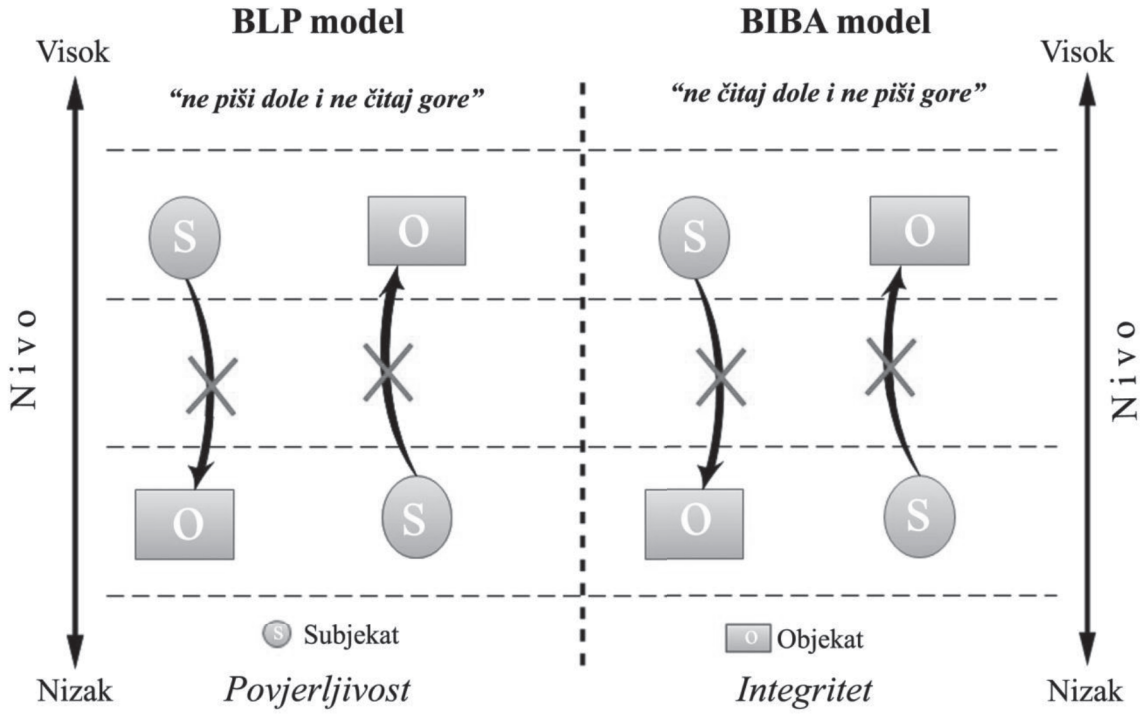
Biba model je razvijen 1977. godine od strane Bibe [4]. Ovaj model je bio prvi model koji se bavio sa pitanjem integriteta u informacionim sistemima. Biba model štiti integritet informacije unutar sistema i veoma je sličan BLP modelu. Nedostaci BLP modela su bili osnovna motivacija za stvaranje Biba modela s ciljem sprečavanje integriteta u kompjuterskim sistemima. Biba model po pitanju informacione zaštite ima dva dijela, prvi koji se bavi podesnim širenjem informacije, dok drugi dio se odnosi prema cjelovitosti ili integritetu informacija. Biba model je fokusiran na obezbijeđivanje mjera integriteta za subjekat i objekat, i sprečavanje nevidljivog uvođenja podataka sa manjim integritetom unutar definisanog sistema. Ovaj model kao i BLP model je takođe zasnovan na informacionom toku u rešetci zaštitnih klasa, sa dopuštenim informacionim tokom samo u jednom pravcu rešetke. Informacioni tok ovog modela je zasnovan na *Low Water Mark* principu, koji dopušta informacioni tok na-dole.

U okviru ovog modela definiše se familija različitih politika koje mogu biti korišćene za primjenu integriteta. Pristup je zasnovan na hijerarhijskoj rešetci nivoa integriteta tj. zasnovan na zaštitnoj klasifikaciji subjekata i objekata gdje je upotrebljen nivo integriteta za klasifikaciju. Dakle, Biba model sprečava neautorizovanu modifikaciju podataka i održavanje konzistentnosti podataka [15]. Ovaj model dodijeljuje subjektima i objektima integritet naljepnicu koja ukazuje u kom stepen je povjerljivost dodijeljena prema informacijama. Sastoji se od četiri pristupna moda: modifikovanja, posmatranja, pozivanja i izvršenja [1]. Biba model podržava pet različitih mandatornih politika integriteta [13]:

1. *Low Water Mark Policy*
2. *Low Water Mark Policy for Objects*
3. *Low Water Mark Integrity Audit Policy*
4. *Ring Policy*
5. *Strict Integrity Policy*

U ovom modelu, tri su diskrecione politike uspostavljene: pristupna kontrol lista, hijararhija objekata i prsten. U praksi, mandatorna politika Biba modela je najčešće korišćena. Najograničenija politika Biba modela je strogo svojstvo integriteta. Upravo, ovo svojstvo integriteta je suštinska suprotnost BLP modela. Strogi model integriteta je sastavljen od tri svojstva. Prvi, jednostavno integritet svojstvo dopušta subjektu da primjećuje (čita) objekat koji ima viši nivo integriteta nego subjekat. Subjekat sa višim nivom integriteta ne može da čita objekat sa nižim nivom integriteta – "*ne čitaj dole*". Drugo, integritet stanja zvjezdanog svojstva je da subjekat ne može modifikovati (pisati) objekat koji ima viši nivo integriteta – "*ne piši gore*". Poslednje, svojstvo pozivanja u kojem subjekat ne smije zahtijevati servis od subjekta koji ima viši nivo integriteta. U ovom modelu su uspostavljene brojne druge politike zasnovane na stanju strogog integriteta. Svaka od tih politika je manje restriktivna nego što je politika strogog integriteta. Model ima brojne dinamične politike koje snižavaju nivo integriteta bilo subjekta ili objekta zasnovanog na operacijama pristupnog moda.

Međutim, kako Biba model radi suprotno od BLP modela, upravo ta činjenica predstavlja glavnu karakteristiku ovog modela jer omogućava njegovu integraciju sa BLP modelom kao i mnogim drugim modelima. Jedan od modela kao što je Lipnerov model integriteta, kombinuje Biba model i BLP model tako što integriše oba principa integritet i povjerljivost [9]. Prednosti Biba modela su jednostavnost i laka primjena, kao i stvaranje i upotreba brojnih različitih politika zasnovanih na potrebi sistema. Glavni nedostatak je što nije jasno kako dodijeljuje odgovarajuće nivoe kao i ne postojanje kriterijuma za određivanje istih. Ovaj model ne podržava principe odobrenja i opoziva autorizacija. Takođe, njegovo ograničenje je što nije striktno korišćen za integritet. Upotreba ovog modela zahtijeva da svi kompjuteri u sistemu moraju imati naljepnicu integriteta za subjekte i objekte. Postoje i drugi problemi u mrežnom okruženju koji ne podržavaju naljepnice integriteta, i sl. Ipak, neki autori poput Sandhu et al. [5] navode da ne postoji fundamentalna razlika između BLP i Biba modela. Komparativni pregled ova dva modela je dat na slici 2.



Slika 2. *BLP naspram Biba modela*

4.3. *The Take-Grant model*

Take – Grant model je diskrecioni model zaštite [6]. Ovaj model kao i prethodni modeli su primarno teoretski alati korišćeni da analiziraju pitanje zaštite. Za razliku od drugih modela, ovaj model predstavlja okvir u kojem je na pitanje zaštite odgovoreno sa "da". Takođe, ovaj model omogućava derivaciju rezultata ukazujući pod kojim pravima mogu biti prenijeti kao i kompleksnost određivanja *da li su ili nisu* ovi uslovi sadržani u partikularnim sistemima. Ovaj model je u suprotnosti prema Biba modelu, koji je uglavnom korišćen da podrži mandatnu politiku koja podržava privilegovanu autorizaciju. Poput Biba modela, Take – Grant model takođe opisuje zaštitu zasnovanu na subjektima i objektima. Ovaj model upotrebljava usmjereni graf da opiše zaštitna stanja. U grafu, subjekti i objekti su prezentovani kao čvorovi kao što je to Bishop predstavio u radu [16]. Pristupni modovi su predstavljeni na ivici koja povezuje čvorove kao što su subjekat prema objektu. Ivice, takođe imaju naljepnice koje formulišu pridružena prava sa tim. Lukovi između čvorova su označeni sa ovim pristupnim pravima. Ovaj model upotrebljava graf za model kontrolnog pristupa; model je fundamentalni model matričnog pristupa [17]. Pristupni modovi koji podržavaju Take – Grant model su čitanje, pisanje, odobrenje i opoziv. U poređenju sa Biba modelom, ovaj model predstavlja prošireni model jer podržava operacije odobrenja i opoziva. Pravo odobrenja/opoziva dopušta subjektu da odobri/oduzme mogućnost pisanja koje subjekt posjeduje prema drugom subjektu ili objektu. Pravo odobrenja i opoziva, takođe poznato kao pravo transfera [1], podržavajući modifikaciju autorizacije sistema koji dopušta pravo da bude prenijeto prema drugom objektu. Transfer prava dopušta subjektu da da ili uzme prava objekta. Na ovaj način savladava se jedan od problema Biba modela, kao što je ne obezbjeđivanje bilo koje administrativne opcije za odobrenje ili opoziv autorizacija [18].

Takođe, Take – Grant model može lako biti primjenjen za zaštitu baze podataka. Neki modeli, kao u slučaju Biba modela, nisu bili razvijeni za zaštitu baza podataka odnosno veoma ih je teško bilo primjeniti u te svrhe. Svojstvo odobrenja ili opoziva autorizacija omogućava da mnogi sistemi koriste ovaj model za autorizaciju privilegija. Na primjer, Orakl upotrebljava *Grant* (odobrenje) komandu da dopusti Oraklu da zna ko autorizuje korisnika ili ulogu, da ima jednu ili više sistema ili objekata privilegija [19]. Sa druge strane, *Revoke* (opoziv) uklanja privilegiju koju korisnik ima na objektu. Sintakse za dvije komande u Oraklu su:

grant <privilege> to <USERNAME or ROLE>
revoke <privilege> from <USERNAME>

Međutim, ni ovaj model nije bez nedostataka. Nedostatak ovog modela u odnosu na Biba model je što ovaj model ne razmatra pitanje integriteta. Takođe, i ovaj model je ranjiv prema trojanacima. Ipak, najveći problem ovog modela je ograničenost u broju čvorova koji mogu biti prikazani u nekom vremenu sa modelom. Grafovi sa velikim brojem čvorova i lukova predstavljaju kompleksan i težak zadatak za pojedinca da shvati i odobri zaštitu.

4.4. *Sea-View Model*

Sea – View Model je razvijen od strane Denning et al. na Istraživačkom institutu Stanfordu. Poput Biba modela, Sea View model koriste mandatnu kao i diskrecionu politiku da

upravlja pristupom prema pohranjenim podacima u bazi podataka. Međutim, za razliku od Biba modela koji se ne bavi sa principom tajnosti, Sea View model kombinuje oba principa, tajnost i integritet. Ovaj model se sastoji od dva sloja. Prvi, kontrolni pristup – MAC (*engl. Mandatory Access Control*) koji je obavezan i odgovara prema odgovarajućem referentnom monitoru koji pojačava mandatnu politikud zaštite BLP modela. Drugi sloj je povjerljivo izračunavanje baze – TCB (*engl. Trusted Computing Base*) i "definiše koncept višestrukog nivoa odnosa, podrške diskrecionih kontrola za višestruke odnose i poglede, i formalizovanje podržavajućih politika" [18].

U MAC modelu, korisniku je dat pristup da klasifikuje informacije zasnovane na korisničkoj dozvoli (autorizacionoj tajnosti i integritetu) za informacije. U ovom modelu mandatna politika je formalizovana u pojmu subjekata, objekata i pristupnih klasa. Takođe, primjenjuju se isti aksiomi koji su korišćeni u BLP i Biba modelu. Pristupne klase i identifikatori dodijeljeni su za cijeli život objekta i sastoje se iz dvije komponente: tajnost i integritet. Klasa tajnosti odgovara prema zaštitnom nivou BLP modela obzirom da klasa integriteta odgovara prema integritetu nivoa Biba modela. Poput Biba modela, *Sea – View* model formira povezanost rešetke. Sličnost ovog modela sa Biba modelom je u tome što su subjekti definisani kao procesi koji djeluju u ime korisnika. Za razliku od Biba modela, svakom korisniku u sistemu koji koristi *Sea – View* model dodijeljeno je područje minimalnih i maksimalnih klasa tajnosti i integriteta u kojem korisniku je dozvoljeno da djeluje. Ove klase su nazvane kao *minzaštita, minitegritet, makszaštita i maksintegritet*. Klase su sastavljene od strane korisnika za pisanje subjekta od para *minzaštita* i *maksintegritet* dok za čitanje od para *makszaštita* i *minintegritet*.

Mandatni pristup modova *Sea – View* modela su: čitaj, piši, i izvršavaj. Operacija čitanja je slična za operaciju opserviranja pristupnog moda kod Biba modela, koji dopušta subjektu da čita informacije pohranjene u objektu. Pristupni mod pisanja dopušta subjektu da piše informacije u objektu, dok mod izvršenja dopušta subjektu da izvrši na objektu. Ovi modovi su uporedivi za operacije modifikovanja i izvršavanja kod Biba modela, za svakog posebno. U svojstvu čitaj, subjekat *i* može čitati objekat *j* samo ako njegova klasa čitanja dominira klasom pristupa objekta. Ovo svojstvo je formulisano *ne čitaj – gore* tajnost BLP modela, i *ne čitaj – dole* integritet Biba modela. U svojstu piši, subjekat *i* može pisati objekat *j* ako njegova klasa pisanja dominira klasom pristupa objekta. Ovo svojstvo je formulisano *ne piši – dole* tajnost BLP modela, i *ne piši – gore* integritet Biba modela. Na kraju, svojstvo izvršenja dopušta subjektu *i* da izvrši objekat *j* samo ako njegov maksimalni integritet je manji ili jednak nego što je to integritet klase objekta, i njegova maksimalna tajnost je veća ili jednaka nego što je to tajnost klase objekta. Ovo svojstvo savladava ograničenja Bibe modela. Stoga, prema Castanu et al. [18], *Sea – View* model izvršava ova svojstva na sljedeći način: "razlikujući pristup izvršenja od pristupa čitanja, dopuštajući povjerljivim subjektima da čitaju podatke manjeg nivoa integriteta nego što je njihov maksimalni integritet, i ograničavaju pristup izvršenja za sve subjekte da programiraju veći ili jednak integritet."

4.5. *Clark – Wilson model*

Clark – Wilson model je razvijen 1987 godine od strane *Clark – Wilson*. U poređenju sa Biba modelom, ovaj model predstavlja prošireno područje održavanja integriteta koji se bavi zaštitom integriteta informacija u svrhu sprečavanja, modifikovanja ili krađe informacija u komercijalnim sistemima. Potrebno je naglasiti da su *Clark – Wilson* u radu [11] pravili jasnu razliku između vojne i komercijalne zaštite. Oni dokazuju da zaštitna politika u pogledu integriteta predstavljaju najviši prioritet u komercijalnim informacionim sistemima za čiju primjenu su potrebni posebni mehanizmi. Dakle, široka upotreba ovog modela je u bankarskim sistemima gdje je integritat važniji nego povjerljivost.

Clark – Wilson predlaže dva nivoa integriteta [10]: *constrained data items – UDIs* (podaci koji su već dio sistema) i *unconstrained data items – UDIs* (podaci koji će biti uvedeni u sistem).

Prema Krause et al. [13] ovaj model definiše tri cilja integriteta:

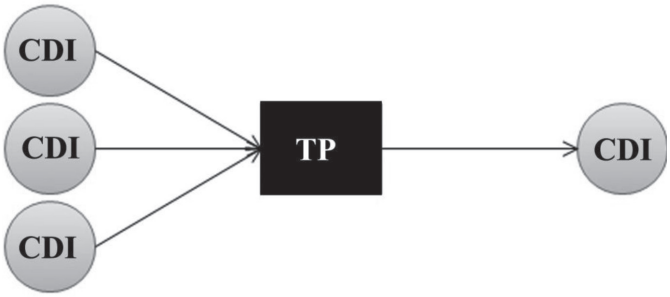
1. Neautorizovani subjekat ne može činiti bilo kakve izmjene,
2. Autorizovani subjekat ne može činiti bilo koje neautorizovane izmjene,
3. Unutrašnja i vanjska postojanost je održana.

U komercijalnom okruženju, ovi ciljevi su pogodni da obezbijede integritet korporativnih finansija podataka ili zapisa. Prednost ovog modela ogleda se u tome što ne samo da je neautorizovanim pojedincima zabranjen pristup zaštićenim podacima, već je i autorizovanim pojedincima zabranjeno činjenje izmjena koje mogu rezultirati u gubljenju ili korupciji finansijskih podataka ili zapisa [13]. Ovaj model ima dva primarna elementa za postizanje integriteta podataka: zahtjev za provjerom (dobro oblikovanu transakciju) i razdvajanje dužnosti [13]. Prema tome, ovaj model je integrisani model primjenjen da zaštiti integritet podataka i da obezbijedi kako se desila ispravno oblikovana transakcija. Dobro oblikovana transakcija je struktuirana tako da subjekt ne može proizvoljno manipulisati podacima, već na ograničen način sa kojim se obezbjeđuje *unutrašnja* konzistentnost podataka. Sa ovim principom je uveden princip dualiteta za svaku transakciju. To podrazumijeva zapis svake transakcije na najmanje dva mjesta čime se ostavlja njen dupli trag. Pri tom je neophodno istaći, da postojanje duplog traga nema za cilj kopiranje transakcija već odvajanje zapisa koji je korišćen da potvrdi tačnost i validnost orginalnih transakcija. Dakle, Clark – Wilson model u poređenju sa Biba modelom dopušta postojanje traga.

Principom razdvajanjem dužnosti sprečava se neodgovarajuća modifikacija podataka od strane autorizovanog korisnika, čime se obezbjeđuje *vanjska* konzistentnost podataka objekta. Drugim riječima obezbjeđuje se korespodencija među objektima podataka različitih poddijelova zadatka. Ova korespodencija je obezbjeđena kod odvajanja svih operacija u nekoliko poddijelova i zahtijevaju da svaki poddio bude izvršen od strane različitog subjekta. Model integriteta ne primjenjuje klasifikacione nivoe za podatke ili korisnike. Umjesto toga, postavlja

se stroga kontrola korisničkog pristupa i upravljanja podacima i programima. Takođe, ovdje je bitno naglasiti da se kroz princip razdvajanja dužnosti obezbjeđuju i dopunski zaštitni zahtjevi u pogledu korisničke identifikacije, autentifikacije i provjere. Clark – Wilson model primjenom principa razdvajanja dužnosti obezbjeđuje integritet podataka kod subjekata na istom ili nižem nivou integriteta, dok je to u Biba modelu bilo zasnovano na pretpostavci da subjekti neće namjerno ili slučajno korumpirati podatke. Dakle, dobro oblikovana transformaciona procedura – TP i integritet verifikaciona procedura – IVP uvedeni su kao sredstvo za osiguravanje ispravnog sistemskog funkcionisanja od jednog stanja do drugog, zasnovanom na jednom ili više ulaza kao što je to prikazano na slici 3 (zasnovano na tri ulaza).

Najčešće TP-s djeluje na skupu CDI-s. Međutim, određeni ovjereni procesi mogu takođe djelovati na skupu UDI-s kako bi uveli podatke u sistem. U takvim situacijama dodijeljuje im se naljepnica CDI-s. Verifikaciona procedura potvrđuje da je verifikacija izvršena kada su podaci prilagođeni prema specifikacijama integriteta u vremenu. Transformacione procedure su dizajnirane da ispravno prevedu sistem iz jednog u drugo stanje. Ipak, *Clark – Wilson* model pretpostavlja pojedinačni visoki nivo integriteta primjenjen prema CDI-s, a model sa eksplicitnijim pravila za upravljanje sistema podataka na nivoima višestrukog integriteta (na primjer Biba modela) mogu biti inkorporisani unutar tog modela [15]. Autori ovog modela su vjerovali da se bave sa sva tri cilja integriteta.



Slika 3. *Dobro formirana TP operativan na tri CDI-s sa kombinovanim izlazom*

U literaturi se može pronaći nekoliko aplikacija i različitosti *Clark – Wilson* modela kao što su [15, 20-23]. Ipak, na kraju je potrebno istaknuti da, ovaj model je kompleksan i ne riješava druga pitanja zaštite [4].

5. DISKUSIJA

U ovom dijelu rada diskutuje se o problemima koji mogu narušiti bazična načela informacione zaštite. Problemi modela zaštite informacija manifestuju se pri njihovoj upotrebi. Prije svega, to su neočekivani problemi koji nastaju pri praktičnoj primjeni nekog modela zaštite. Dakle, modeli zaštite imaju teoretska ograničenja. Ne može se uvijek dokazati da model zadovoljava određeni uslove zaštite. Praktično, primjenom određenog modela zaštite pojavljuju se problemi koji nisu teoretski mogli biti identifikovani. Sa druge strane, modeli zaštite zasnovani na strogim matematičkim svojstvima mogu da vode ka sistemima koji su potpuno neupotrebljivi. Razvijanje sistema zasnovanih na strogim matematičkim modelima zaštite je ekstremno vremenski zahtijevan i veoma skup proces. Ovakvi modeli zaštite nisu ekonomski isplativi i stoga većina komercijalnih sistema neće biti zasnovana na formalnim modelima. Modeli zaštite i formalne metode ne omogućavaju uspostavljanje zaštite sistema. U slučajevima, ako bi dokazljivost bazičnog principa zaštite i bila moguća, to nije prihvatljivo rješenje. Razlog je što model zaštite u trenutku testiranja može da potvrdi sigurnost sistema, dok već u sledećem testiranju može pokazati određene ranjivosti.

Nesumnjivo, da čovjek predstavlja najveću prijetnju i ranjivost bilo kog modela zaštite. Ljudski faktor i socijalni inženjering mogu da kompromituju i najzaštićenije sisteme. Takođe, kontinuirani napredak digitalnih tehnologija stvorio je uslove za razvoj novih oblika prijetnji po modele zaštite. Brz i snažan razvoj digitalnih tehnologija uslovio je da zaštitni mehanizmi za koje se mislilo u određenom vremenu da su sigurni u bliskoj budućnosti se pokazalo da su potpuno nesigurni. Primjer za ovo su kriptografski algoritmi. Zbog snažnog razvoja procesorske moći kompjutera, algoritmi poput DES koji su po razvijanju smatrani najsigurnijim algoritmima u veoma kratkom periodu nisu se mogli više smatrati sigurnim. Sa razvojem procesorskih kompjuterskih perfomansi takvi algoritmi su u kratkom vremenskom periodu bili razbijani. Bez obzira, kako zaštita sistema je odobrena da bude model, sistem je izložen kontinuiranom riziku od moguće zloupotrebe.

Nesumnjivo je da *Clark – Wilson* model obezbjeđuje opšti okvir u kojem je moguće upravljati integritetom podataka primjenom strogog vodiča. Međutim, ovaj model u poređenju sa Biba modelom dopušta za procese da djeluju na višestrukim izvorima podataka ali nijedan od modela ne razmatra kako postojanje višestrukih izvora povezanih podataka mogu uticati na njihov nivo dodijeljenog integriteta. Na primjer, neki dio podatka može povećati ili smanjiti nivo integriteta drugog podatka zasnovanog na tom da li je podatak potvrđen ili kontradiktoran, i zasnovanog na stepenu nezavisnosti izvora podataka. Nadalje, modeli ne obuhvataju kontekstualne informacije kod kojih je nezavisnost zaključena.

6. ZAKLJUČCI

U ovom radu je dat pregled, opis i komparacija osnovnih modela zaštite kao što su *Bell–LaPadula, Biba, Take–Grant, Sea–View* i *Clark–Wilson* model. U tom komparativnom metodu istražene su neke od sličnosti i različitosti između postojećih osnovnih modela zaštite. Zbog svojih povoljnih integracionih karakteristika, jednostavnosti i primjene *Biba* model je poslužio kao bazični model za poređenje. U slučaju *Biba* modela, neke politike su restriktivnije nego druge. Na primjer, *low-water mark* politike su dinamičnije i nižeg nivoa integriteta subjekta i objekta, koji rezultuju u modelu da je lakši za upotrebu ali sa manjim nivoom zaštite. Sa druge strane, Take–Grant model podržava autorizaciju privilegija koje su kod Biba modela prigušene.

Takođe, u ovom radu došlo se do zaključka, da i pored brojnih razvijenih modela zaštite, ne postoji savršen model tj. model koji u isto vrijeme pokriva sve bazične aspekte zaštite. Kako je kompjuterska zaštita uvijek dio reakcionog procesa, potpuno je svejedno koji će model zaštite biti primjenjen, problemi će uvijek iznova iskrsavati. Ukoliko jedan model zaštite ima nedostatke u određenom pravcu, u drugom modelu koji se pojavi kao korektura, obavezno se javljaju problemi druge prirode. Razlozi mogu biti uzrokovani ljudskim faktorom kao i ubrzanim razvojem digitalnih tehnologija. Nesumnjivo, prijedlog za ublažavanje identifikovanih problema je usmjeren prema stvaranju odgovarajućih alata koji će značajno onemogućiti ili odvratiti napadače u namjerama zloupotrebe informacija. Za praktičnu primjenu zaštite informacija u većini slučajeva potrebna je primjena više od jednog modela zaštite.

LITERATURA

[1] Balon, I. and Thabet, I. Biba security model comparison. CIS 576, 2004.

[2] Alharby, N. E-government Security: Explaing Main Factors and Analysing Existing Models. World Academy of Science, Engineering and Technology International Journal of Social, Human Science and Engineering 7(9), pp. 1319-1321, 2013.

[3] Bell, D.E. and LaPadula, L. Secure Computer Systems: Unified Exposition and Multics Interpretation. ESD-TR-75-306, MITRE MTR-2997, MITRE Corporation, 1976.

[4] Biba, K.J. Integrity constraints for secure computer systems. Technical Report EST TR-76-372, Hanscom AFB, 1977.

[5] Sandhu, R.S. and Mason, G. Lattice-based Access Control Models. IEEE, pp. 9-19, 1993

[6] Lipton, R. J. and Snyder, L. "A linear time algorithm for deciding subject security." Journal of the ACM, 24(3):455-464, 1977.

[7] Denning, D. E., Lunt T.F., Schell, R. R., Shockley, W.R., and Heckman M. The sea view security model. IEEE, pp. 218-233, 1998.

[8] Brewer, D. F. C. and Nash, M. J., The Chinese Wall security policy. *IEEE Symp. on Security and Privacy,* 1989, pp. 215-228.

[9] Lipner, S. B. Non-discrentionary controls for commercial applications. In IEEE Symposium on Security and Privacy, pp. 2-10, Oakland, May 1982.

[10] Anderson, M., Montague, P. and Long, B. A Formal Integrity Framework with Application to a Secure Information ATM (SIATM). DSTO Defence Science and Technology Organisation. Commonwealth of Australia 2012.

[11] Clark, D. D. & Wilson, D. R., A comparison of commercial and military computer security policies, in IEEE Symposium of Security and Privacy, pp. 184-194, (1987)

[12] Braghin, C., Sharygina, N. and Barone-Adesi, K. A Model Checking-based Approach for Security Policy Verification of Mobile Systems. Formal Aspects of Computing, 23(5), pp. 627-648, 2010.

[13] Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition, vol.2, Taylor & Francis Group, 2005.

[14] Stamp, M. Information Security Principles and practice. John Wiley & Sons, Inc., Hoboken, New Jersey. 2006.

[15] Bishop, M. Computer Security: Art and Science, Addison Wesley, Boston, MA. 2003.

[16] Bishop, M. "Hierarchical Take-Grant Protection System" Proceedings of the eighth ACM symposium on Operating systems principles. Pacific Grove, California, pp. 109 – 122, 1981.

[17] Landwehr, C. "Formal Models for Computer Security", Computing Surveys, Vol. 13, No. 3, September 1981.

[18] Castano, S., Fugini, M., Martella, G., and Samarati, P. Database Security, Addison Wesley, Harlow, England. 1995.

[19] Therialut, M. & Newman, A. Oracle Security Handbook: Implementing a Sound Security-Plan in Your Oracle Environment. McGraw-Hill, Berkeley, CA. 2001.

[20] Hanigk, S. Con_dentiality is not enough: A multi-level Clark-Wilson model for network management, in MilCIS 2009.

[21] Zhou-Yi, Z., Ye-Ping, H. & Hong-Liang, L. Hybrid mandatory integrity model composed of Biba and Clark-Wilson policy, Ruan Jian Xue Bao (Journal of Software) 21(1), pp. 98-106, 2010.

[22] Qingguang, J., Sihan, Q. & Yeping, H. A formal model for integrity protection based on DTE technique, Science in China Series F: Information Sciences 49, pp. 545-565, 2006.

[23] Ge, X., Polack, F. & Laleau, R. Secure databases: an analysis of Clark-Wilson model in a database environment, in Advanced Information Systems Engineering -16th International Conference, CAiSE 2004, pp. 7-11, 2004.

Mr Dragan Korać, Univerzitet u Beogradu – Fakultet organizacionih nauka, student doktorskih studija.
Kontakt: korac@teol.net
Oblasti interesovanja: sigurnost, zaštita podataka i računarskih sistema, informacioni sistemi, mobilne tehnologije i fazi logika