SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 2:

Sigurnosne arhitekture i modeli

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Sigurnosne arhitekture i modeli

- Sadržaj predavanja:
  - 2.1. Osnove sigurnosnih arhitektura
  - 2.2. Pojam i problem bezbednosti i modeli sigurnosti

*"*Security Architecture & Models is one of 10 domains comprising the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK)."*

"Our plans miscarry because they have no aim. When a man does not know what harbor he is making for, no wind is the right wind."

Seneca

Potrebna predznanja

- Za detaljnije proučavanje formalne teorije sigurnosnih arhitektura i modela potrebno je predznanje iz sledećih oblasti:
  - Računarske arhitekture
    - Sabirnica (engl. bus)
    - Centralni procesor, CPU
    - Memorija
    - Ulazno izlazni podsistem
    - Periferni uređaji
  - Operativni sistemi
  - Softver
  - Programski jezici i programiranje
  - ...

2.1 Osnove sigurnosnih arhitektura

- Sistemi:
  - Otvoreni
  - Zatvoreni
  - Centralizovani
  - Distribuirani

Sigurnosna arhitektura

- **Sigurnosna arhitektura** informacionog sistema - osnovu za sprovođenje sigurnosne politike svake organizacije.

- Zavisi od toga o koliko strogoj sigurnosnoj politici je reč i o kakvom se sistemu radi – zatvorenom ili otvorenom, centralizovanom ili distribuiranom

Poverenje i perimetar

- **Računarska baza od poverenja** (engl. *Trusted Computing Base, TCB*) celovita je kombinacija zaštitnih mehanizama unutar računarskog sistema, koja uključuje hardver, softver i firmver, i za koju se veruje da obezbeđuje primenu sigurnosnih pravila.

- **Sigurnosni perimetar** (engl. *security perimeter*) predstavlja granicu koja odvaja TCB od ostatka sistema. Mora postojati i **nerizičan put** (engl. *trusted path*) koji obezbeđuje korisniku da pristupi TCB-u tako da ga pri tome ne mogu kompromitovati drugi procesi i/ili korisnici.

- **Računarski sistem od poverenja** (engl. *trusted computer system*) jeste onaj računarski sistem koji koristi nužne mere obezbeđenja hardvera i softvera kako bi omogućio obradu informacija klasifikovanih na više nivoa. Ovaj sistem treba da zadovolji specificirane zahteve u pogledu pouzdanosti i sigurnosti.

Apstrakcija i koncept skrivanja informacija

- **Apstrakcija** (engl. *abstraction*) znači posmatranje sistemskih komponenti na višem nivou, odnosno ignorisanje njihovih specifičnih detalja na nižem nivou

- **Sakrivanje informacija** (engl. *information hiding*) koristi se recimo u objektno-orijentisanom programiranju

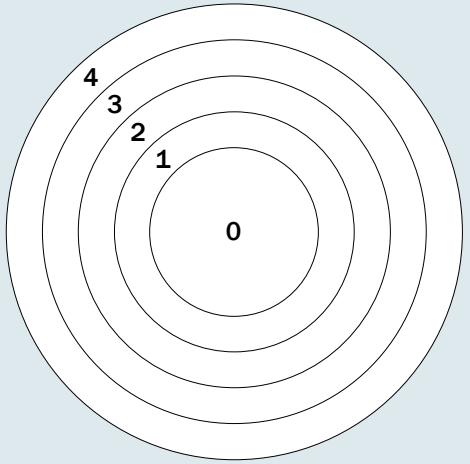
Domeni zaštite i zaštitni prstenovi

- Svaki proces ima pristup određenim memorijskim lokacijama i mogućnost da izvršava podskup računarskih instrukcija. Izvršavanje procesa i memorijsko područje koje je dodeljeno svakom procesu zove se **zaštitni domen** (engl. *protection domain*).

Zaštitni prstenovi

- Jedna od šema koja podržava višestruke domene zaštite jeste korišćenje **zaštitnih prstenova** (engl. *protection rings*).

- Prstenovi su realizovani tako da je domen sa najvećim pravima u centru prstena, a da je domen sa najmanjim pravima spoljašnji, tj. periferni prsten.



Sigurno jezgro

- **Sigurno jezgro** (engl. *security kernel*) čine hardverski, firmverski i softverski elementi računarske baze od poverenja, koji implementiraju koncept **monitora referenci** (engl. *reference monitor*). Monitor referenci je sistemska komponenta koja forsira kontrolu pristupa objektima. Monitor referenci je apstraktna mašina koja je posreduje svaki put kada neki subjekat pristupa objektima.

- Sigurno jezgro mora da:
  - posreduje u svim pristupima
  - bude zaštićeno od izmena
  - bude verifikovano kao ispravno

Sigurno jezgro...

- Postoje i drugi pristupi zaštiti, zasnovani na jezgru i srodnim mehanizmima:
  - korišćenje posebnog hardverskog uređaja koji proverava sve reference u sistemu i objavljuje ih za važeće;
  - implementiranje monitora virtuelne mašine (engl. *virtual machine monitor*), koji uspostavlja brojne virtuelne mašine, koje su izolovane jedna od druge. Svaka mašina može da se izvršava na različitom sigurnosnom nivou;
  - korišćenje softverski sigurnog jezgra koje radi u vlastitom domenu zaštite.
- Namena virtuelnih mašina je formiranje velikog broja odvojenih identičnih izvršnih okruženja na jednom računaru.

Sigurnosne oznake

- **Sigurnosna oznaka** (engl. *security label*) se dodeljuje nekom resursu. Sigurnosna oznaka može ukazati na potrebu za posebnim načinom (odnosno režimom) rukovanja (rukovanje objektom uz primenu dodatnih sigurnosnih mehanizama), ili se može koristiti za kontrolu pristupa.

Sigurnosni režimi

- Informacioni sistemi rade u različitim sigurnosnim režimima koji su određeni nivoima klasifikacije informacija, kao i profilima korisnika i njihovim ovlašćenjima (engl. *clearance*).

Režim rada sa više nivoa

- Namenski (engl. dedicated)
  - Svi korisnici imaju ovlašćenja i potrebu da znaju sve informacije koje obrađuje informacioni sistem; sistem može da radi sa više klasifikacionih nivoa.
- Odeljeni (engl. *compartmented*)
  - Svi korisnici imaju ovlašćenja za najviši nivo klasifikovanih informacija, ali oni ne moraju imati ovlašćenje i potrebu da znaju sve podatke koji se nalaze ili obrađuju u računarskom sistemu.
- Kontrolisani (engl. *controlled*)
  - Tip sigurnosti ostvarene sa više nivoa gde je određeni ograničeni nivo poverenja ostvaren pomoću sistemske hardversko – softverske osnove, zajedno sa odgovarajućim ograničenjima u pogledu nivoa klasifikovanih informacija koje se mogu obrađivati.
- Ograničeni pristup (engl. *limited access*)
  - Sistem u kome rade korisnici nisu sigurnosno provereni, gde je maksimalan stepen tajnosti podataka: neklasifikovani, ali osetljivi.

Distribuirane arhitekture

- Migracija od centralizovanih modela računarskih sistema ka klijent / server modelu i ka višeslojnim modelima, stvorila je nov skup problema za profesionalce u oblasti sigurnosti informacionih sistema. Situacija se dodatno zakomplikovala sve većom primenom stonih i prenosnih računara. Na tim računarima mogu se nalaziti dokumenti koji su osetljivi za posao kojim se bavi neka organizacija, a mogu biti i ugroženi.

Ranjivosti u sigurnosnoj arhitekturi

- Ranjivosti (engl. *vulnerability*) u sistemskoj sigurnosnoj arhitekturi mogu voditi ka naraušavanju sistemske sigurnosne politike.
- Tipične ranjivosti:
  - Skriveni kanal (engl. *covert channel*)
  - Nepostojanje provere perimetra (engl. *lack of perimeter checking*)
  - „*Maintenance hook*“ ranjivost
  - *Time of Check to Time of Use*“ (TOC/TOU) napad

Procedure oporavka

- Kada dođe do greške hardverske ili softverske komponente sistema od poverenja, veoma je važno da ta greška ne kompromituje zahteve sigurnosne politike tog sistema.

- Režim održavanja (engl. *maintenance mode*)
- Sistem otporan na greške (engl. *fault-tolerant system*)
- Sistem bezbedan u slučaju otkaza (engl. *fail-safe system*)
- Sistemu elastičan u slučaju otkaza (engl. *resilient*), tj. „*fail-soft*“

- Izraz „*fail-over*“ odnosi se na prebacivanje na „vruću“ rezervnu komponentu (engl. *hot backup*) u realnom vremenu kada se desi i otkrije hardverska ili softverska greška, što omogućava da sistem nastavi rad

Kriterijumi ocenjivanja, sertifikacija i akreditacija

- 1985, Nacionalni centar za računarsku sigurnost (*National Computer Security Center*, NCSC) razvio je kriterijum za procenu računarskih sistema od poverenja (*Trusted Computer System Evaluation Criteria*, TCSEC). TCSEC pruža sledeće:
- osnovu za uspostavljanje zahteva u pogledu sigurnosti u procesu definisanja specifikacija
- standard za sigurnosne usluge koje proizvođači treba da obezbede za različite klase sigurnosnih zahteva
- načine i sredstva za merenje pouzdanosti i poverljivosti, tj. stepena poverenja koji se može ukazati informacionom sistemu.

Kriterijumi ocenjivanja, sertifikacija i akreditacija...

- TCSEC dokument, nazvan Narandžasta knjiga (*Orange book*) deo je serije smernica objavljenih u knjigama sa koricama različitih boja koja se zove Dugina serija (*Rainbow series*). Narandžasta knjiga definiše osnovne hijerarhijske klase sigurnosti od slova D do slova A:
- **D. minimalna zaštita** (engl. *minimal protection*)
- **C. diskreciona zaštita** (engl. *discretionary protection*) – klase C1 i C2
- **B. obavezna zaštita** (engl. *mandatory protection*) – klase B1, B2 i B3
- **A. verifikovana zaštita** (engl. *verified protection*); formalne metode (A1)

Kriterijumi ocenjivanja, sertifikacija i akreditacija...

- Dokument *Trusted Network Interpretation* (**TNI**) američkog ministarstva odbrane (*Department of Defense*, *DoD*) analogan Narandžastoj knjizi. Bavi poverljivošću i integritetom u poverljivom računarsko-komunikacionom sistemu i zove se Crvena knjiga (*Red book*). *Trusted Data Base Management System Interpretation* (TDI) obrađuje poverljive sisteme za upravljanje bazama podataka.
- *European Information Technology Security Evaluation Criteria* (**ITSEC**) bavi se poverljivošću, integritetom i raspoloživošću. Proizvod ili sistem koji će biti evaluiran preko ITSEC-a definiše se kao cilj procene (engl. *Target of Evaluation*, TOE). TOE mora imati sigurnosni cilj, koji uključuje i mehanizme za primoravanje i sistemsku sigurnosnu politiku.

Zajednički kriterijum (engl. *Common Criteria*)

- TCSEC, ITSEC, i *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) evoluirali su u jedan kriterijum procene koji se zove **Zajednički kriterijum**.

- Zajednički kriterijum (*Common Criteria*, CC) predstavlja rezultat napora da se razviju kriterijumi za proveru i vrednovanje IT sigurnosti koji će moći da se koriste u međunardnoj zajednici.

- Ujednačavanja velikog broj različitih izvornih kriterijuma: postojećih evropskih (ITSEC), američkih (TCSEC) i kanadskih kriterijuma (CTCPEC). Zajednički kriterijum je opisan u dodatku A.

Sertifikacija i akreditacija

- Sertifikacija (engl. *certification*) je opsežna procena tehničkih i netehničkih sigurnosnih karakteristika informacionog sistema i drugih zaštitnih mehanizama, koje treba da podrže proces akreditacije.

- Akreditacija (engl. *acreditation*) je formalna deklaracija koju daje ovlašćena organizacija (engl. *Designated Approving Authority*, DAA) i kojom je informacionom sistemu odobreno da radi u određenom sigurnosnom režimu uz korišćenje propisanog skupa mehanizama zaštite i prihvatljiv nivo rizika.

DITSCAP i NIACAP

- Proces sertifikacije i akreditacije sigurnosti odbrambenih informacionih tehnologija - DITSCAP (*Defense Information Technology Security Certification and Accreditation Process*)

- Proces sertifikacije i akreditacije državnih informacionih tehnologija (*National Information Assurance Certification and Accreditation Process*, NIACAP).
  - Akreditacija lokacije (engl. *site accreditation*)
  - Akreditacija tipa (engl. *type accreditation*)
  - Akreditacija sistema (engl. *system accreditation*)

2.2 Pojam i problem bezbednosti i modeli sigurnosti

- Razlika između pojmova bezbednost i sigurnost sastoji se u sledećem:
  - Pojam **bezbednost** (engl. *safety*) odnosi se na apstraktni model.
  - **Sigurnost** (engl. *security*) se odnosi na aktuelnu implementaciju.
  - Siguran sistem odgovara modelu koji je bezbedan u odnosu na sva prava.
  - Međutim, model bezbedan u odnosu na sva prava ne garantuje siguran sistem.

Generalno pitanje

- Kako, za dati računarski sistem, možemo odrediti da li je on siguran?
  - Postoji li generički algoritam koji nam omogućava da odredimo da li je račuarski sistem siguran?
- Šta podrazumevamo pod terminom “siguran”?
  - Da li je to, na primer, korišćenje matrice pristupa da prikažemo politiku zaštite?

Safety

- Let *R* be the set of generic (primitive) rights of the system
  - No special rights copy and own
- **Definition:** when a generic right *r* is added to an element of the access control matrix not already containing *r*, that right is said to be *leaked*
- **Definition:** If a system can never leak right *r*, the system is called safe with respect to the right *r*. If the system can leak right *r*, the system is called unsafe with respect with the right *r*

Safety vs. Security

- Safety refers to the abstract model and security refers to the actual implementation
  - A secure system corresponds to a model safe with respect to all rights
  - A model safe with respect with all rights does not ensure a secure system

The Safety Question

- Does there exist an algorithm for determining whether a given protection system with initial state s_0 is safe with respect to a generic right *r*?

Basic Results

- **Theorem:** There exists an algorithm that will determine whether a given *mono-operational* protection system with initial state s_0 is safe with respect to a generic right *r*

  - **Proof sketch:** Each command is identified by the primitive operation it invokes. Consider the minimal sequence of commands needed to leak *r* from the system with initial state s_0. We can show that the length of this sequence is bounded. Therefore, we can enumerate all possible states and determine wither the system is safe.

Basic Results (cont'd)

- **Theorem:** It is undecidable whether a given state of a given protection system is safe for a given generic right
  - **Proof sketch:** we show that an arbitrary Turing machine can be reduced to the safety problem, with the Turing machine entering a final state corresponding to the leaking of a given generic right. Then if the safety problem is decidable, we can determine when the Turing machine halts. Since we already know that the halting problem is undecidable, the safety problem can't be undecidable either.
- Article on **Turing Machines** from the Stanford Encyclopedia http://plato.stanford.edu/entries/turing-machine/

Basic Results (cont'd)

- The safety problem is undecidable for generic protection models but is decidable if the protection system is restricted in some way

Modeli sigurnosti informacija

- **Modeli kontrole pristupa** (engl. *access control models*)
  - Bell-LaPadula model,
  - Model matrice pristupa (engl. *access matrix*) i
  - Model preuzmi-dodeli (engl. *take-grant model*)
- **Modeli integriteta,** tj. celovitosti (engl. *integrity models*)
  - Biba model integriteta,
  - Clark-Wilson model integriteta
- **Modeli toka informacija** (engl. *information flow models*)
  - Model bez preplitanja (engl. *non-interference* model),
  - Teorije kompozicije (engl. *composition theories*).

Modeli kontrole pristupa

- **Bell-LaPadula** (BLP) model
- **Model matrice pristupa**
  - Matrica pristupa (engl. *access matrix*)
- **Model preuzmi-dodeli** (engl. *take-grant model*)

Bell-LaPadula (BLP) model

- BLP je formalni **model tranzicije stanja** (konačni automat) koji opisuje skup prava za kontrolu pristupa korišćenjem sigurnosnih oznaka na objektima, od najosetljivijih u pogledu tajnosti, do onih najmanje osetljivih, sa sledećom kategorizacijom:
  - strogo poverljivo (engl. *top secret*),
  - tajna (engl. *secret*),
  - poverljivo (engl. *confidential*),
  - neklasifikovano (engl. *unclassified*).
- Bell-LaPadula model se fokusira na **poverljivost** klasifikovanih informacija, za razliku od Biba modela integriteta, koji opisuje pravila za zaštitu integriteta informacija.

Bell-LaPadula (BLP) model…

- Model definiše dva obavezna pravila za kontrolu pristupa i jedno diskreciono pravilo kontrole pristupa sa tri sigurnosna svojstva:

[1] **jednostavno svojstvo sigurnosti** (engl. *simple security property*). Subjekat određenog nivoa poverljivosti ne može čitati objekat koji je na višem nivou poverljivosti, tj. nema čitanja prema gore (engl. ***no read-up***);

[2] **zvezdica (*) svojstvo sigurnosti** (engl. * *(star) security property*). Subjekat određenog nivoa poverljivosti ne može pisati ni u jedan objekat na nižem nivou poverljivosti, tj. nema pisanja prema dole (engl. ***no write-down***);

[3] **diskreciono svojstvo sigurnosti** (engl. *discretionary security property*) koristi matricu pristupa da specificira diskreciona prava.

Model matrice pristupa

- **Matrica pristupa** (engl. *access matrix*) predstavlja jednostavan pristup koji obezbeđuje prava pristupa subjektima za pristup i korišćenje objekata (na primer, pravo čitanja, upisa ili izvršavanja). Subjekat je aktivni entitet – korisnik, program ili proces koji traži prava za pristup i korišćenje resursa ili objekta. Objekat je pasivni entitet – na primer, datoteka ili neki resurs za smeštanje podataka. U nekim slučajevima, jedan entitet tj. stavka može biti subjekat u jednom kontekstu, a objekat u drugom kontekstu.

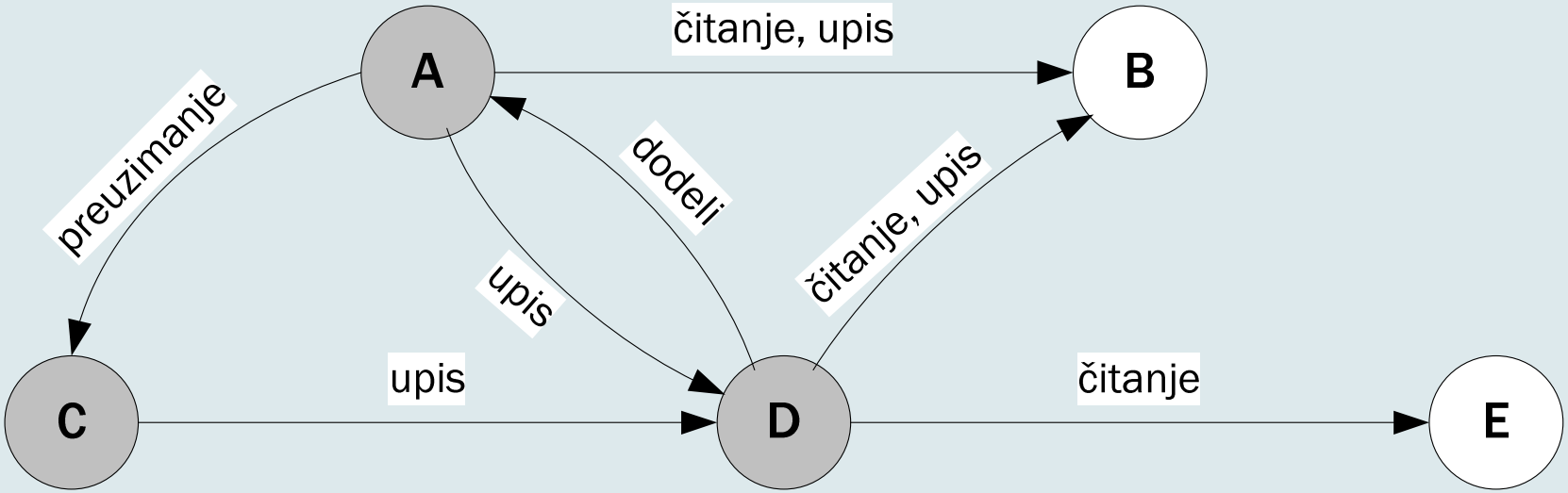
- Kolone matrice pristupa obično se zovu **liste kontrole pristupa** (engl. *access control lists*, *ACLs*), a vrste se zovu **liste mogućnosti** (engl. *capability lists*)

Model preuzmi-dodeli

- Model **preuzmi-dodeli** (engl. *take-grant model*) zasnovan je na modelu matrice pristupa, s tim što je kontrola pristupa predstavljena usmerenim grafovima.
  - **Čvorovi grafa** mogu biti subjekti (na primer, procesi) i objekti (na primer, resursi).
  - **Grana grafa** usmerena od čvora A ka čvoru B znači da subjekat A ima neko pravo nad subjektom (ili objektom) B; grana se obeležava skupom prava koje A ima nad B.

- Model preuzmi-dodeli nudi četiri različita prava pristupa:
  - **Čitanje** (engl. *read*), koje omogućava čvoru A da pristupi čvoru B bez mogućnosti izmene sadržaja,
  - **Upis** (engl. *write*), koji omogućava čvoru A da nešto upiše u čvor B,
  - **Preuzimanje** (engl. *take*), koje omogućava čvoru A da preuzme prava pristupa koja čvor B ima nad nekim drugim subjektom ili objektom, i
  - **Dodela** (engl. *grant*), koja omogućava čvoru A da svoja prava pristupa nad nekim drugim subjektom ili objektom prenese čvoru B.

Primer modela preuzmi-dodeli



Model preuzmi-dodeli - graf

- Grane grafa se mogu dodati i ukloniti primenom prava preuzimanja i dodele.
- Pomoću pravila **„napravi“** (engl. *create*) može se dodati nov čvor u graf. Ukoliko subjekat A pravi čvor B, u graf se osim čvora B dodaje i grana A-B koja sadrži potpuni skup prava pristupa; to znači da subjekat koji pravi neki čvor ima sva prava nad njim.
- Pomoću pravila **„ukloni“** (engl. *remove*) mogu se ukloniti određena prava iz neke grane grafa. Ukoliko su iz neke grane uklonjena sva prava u odnosu na neki čvor, grana se takođe uništava.

Modeli integriteta

- U ovim modelima integritet podataka je važniji nego poverljivost.

- Primeri:
  - **Biba model integriteta**
  - **Model Clark-Wilson**

Biba model integriteta

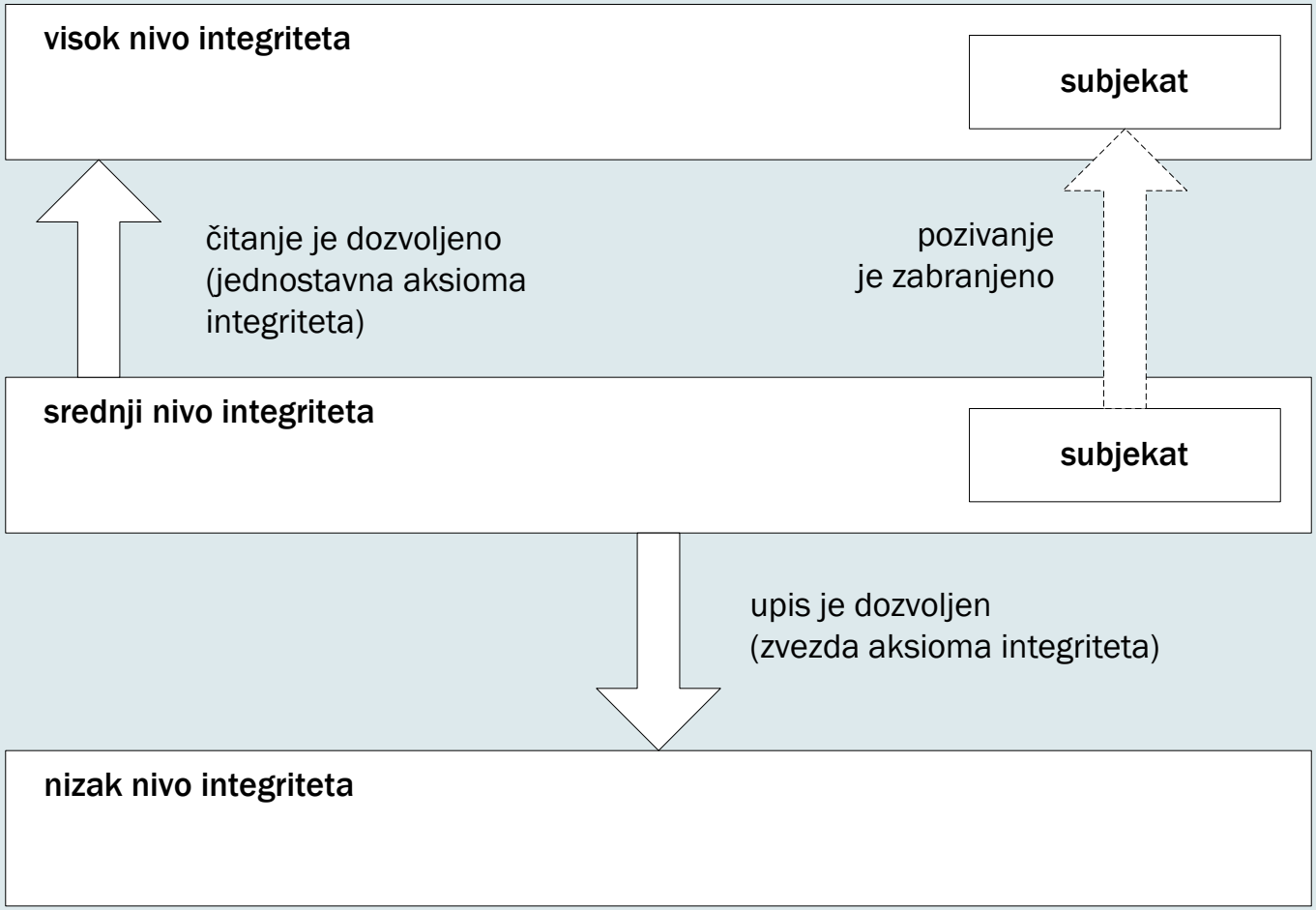
- Biba model integriteta analogan Bell-LaPadula modelu poverljivosti
- Slično klasifikaciji različitih nivoa osetljivosti u Bell-LaPadula modelu, Biba model klasifikuje objekte u različite nivoe integriteta. Model specificira sledeće tri aksiome integriteta:

[1] **Jednostavna aksioma integriteta** (engl. *simple integrity axiom*). Kaže da subjektu na jednom nivou integriteta nije dozvoljeno da vidi (čita) objekat nižeg integriteta (nema čitanja nadole – engl. *no read down*).

[2] **Zvezda (*) aksiom integriteta** (engl. *star integrity axiom*). Kaže da objektu na jednom nivou integriteta nije dozvoljeno da izmeni tj. modifikuje objekat višeg nivoa integriteta niti da upisuje u njega (engl. *no write up*)

[3] Subjekat na jednom nivou integriteta **ne može pozivati** (engl. *invoke*) **subjekat na višem nivou** integriteta.

Biba model integriteta



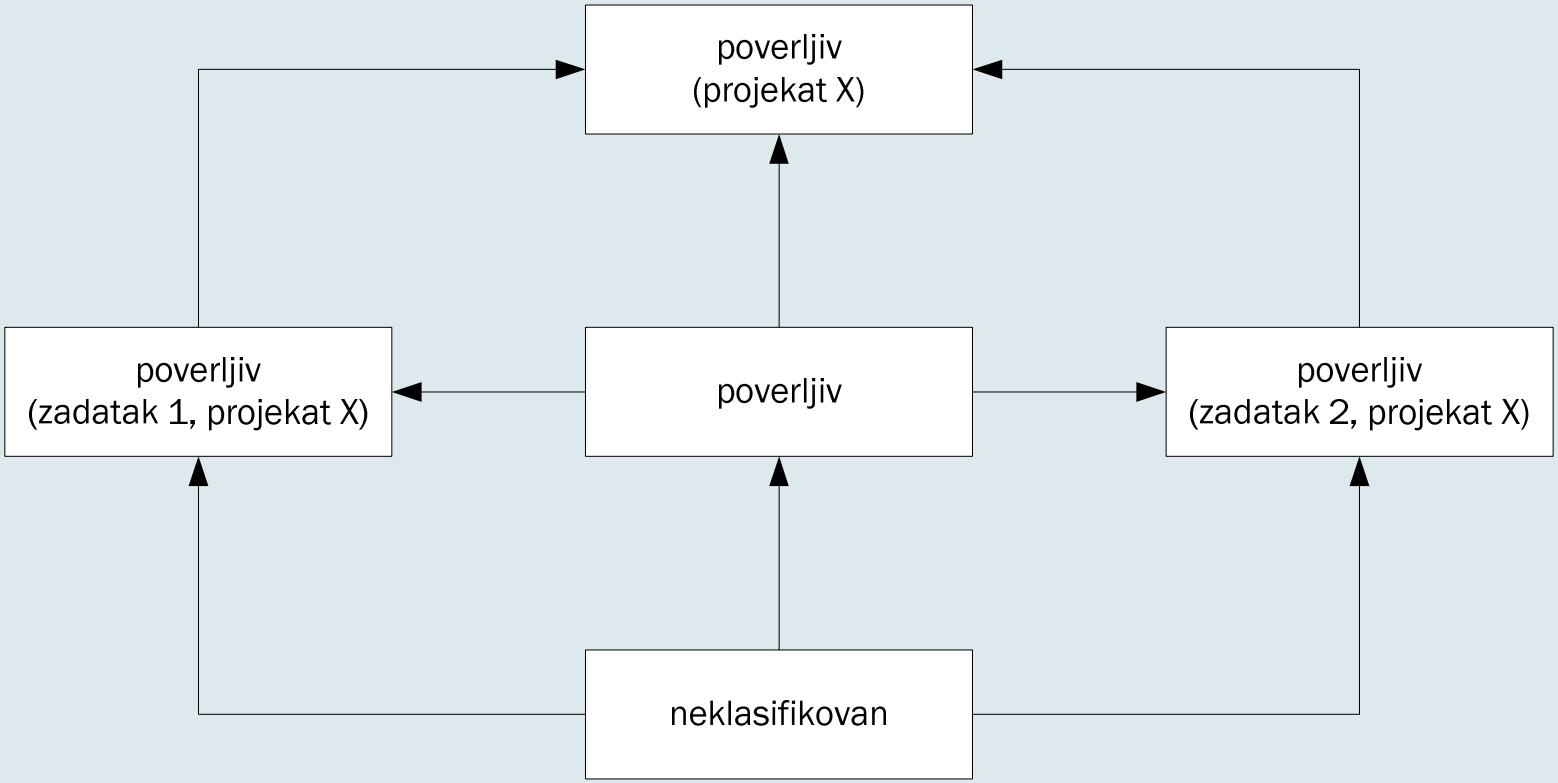
Model Clark-Wilson

- Pristup u modelu Clark-Wilson (1987) sastojao se u tome da se razvije okvir za primenu u realnom komercijalnom okruženju. Ovaj model je okrenut ka tri cilja u pogledu integriteta i definiše sledeće termine:
  - **sputana jedinica podataka** (engl. *constrained data item*, CDI). Jedinica podataka čiji integritet treba da bude sačuvan;
  - **procedura provere integriteta** (engl. *integrity verification procedure*, IVP). Potvrđuje da li su sve CDI jedinice u validnom stanju integriteta;
  - **transformaciona procedura** (engl. *transformation procedure*, TP). Manupuliše CDI-jima kroz dobro formirane transakcije, koje transformišu CDI iz jednog validnog stanja integriteta u drugo.
  - **nesputana jedinica podataka** (engl. *unconstrained data item*). Jedinice podataka koje su van kontrolisanog područja modeliranog okruženja, kao što su ulazne informacije.

Modeli toka informacija

- Tok podataka se zasniva na **konačnom automatu** (engl. *state machine*) i sastoji se od objekata, tranzicija stanja i mreže stanja (polisa tokova). U ovom kontekstu, objekti takođe mogu predstavljati korisnike. Svakom objektu je dodeljena klasa sigurnosti i vrednost, a tok informacija je ograničen na smerove koji su dozvoljeni sigurnosnom politikom.

Modeli toka informacija…



Modeli toka informacija…

- **Model bez interferencije** (engl. *non-interference model*)
- **Kompozitne teorije** (engl. *composition theories*)

Model bez interferencije

- **Model bez interferencije** (engl. *non-interference model*) je u vezi sa prethodno pomenutim modelom toka informacija, ali sa ograničenjima u pogledu toka informacija. Osnovni princip ovog modela je da grupa korisnika (A), koji upotrebljava komande (C) ne ometa grupu korisnika (B), koji upotrebljavaju komande (D). Ovaj koncept se zapisuje kao:

  - A, C:| B, D

Drugim rečima, akcije Grupe A koja koristi komande C ne vide korisnici u Grupi B koji upotrebljavaju komande D.

Kompozitne teorije

- U mnogim primenama i aplikacijama, sistemi su izgrađeni kombinovanjem manjih sistema. Za razmatranje je zanimljiva sledeća situacija: da li su sigurnosna svojstva komponenata sistema održana kada su one kombinovane u obliku većeg entiteta. John McClean je analizirao ovaj problem 1994. godine i tada je definisao dve kompozitne konstrukcije – spoljašnju (engl. *external*) i unutrašnju (engl. *internal*). Definisani su sledeći tipovi spoljašnjih konstrukata:

  - **Kaskadiranje** (engl. *cascading*). Ulaz jednog sistema se dobija kao izlaz drugog sistema;
  - **Povratna sprega** (engl. *feedback*). Jedan sistem obezbeđuje ulaz za drugi sistem, koji na povratku daje ulaz u prvi sistem;
  - **„*Hookup*“**. Sistem koji komunicira s drugim sistemom, a i sa spoljašnjim entitetima;

  Interne kompozicije konstrukata su: presek (engl. *intersection*), unija (engl. *union*) i razlika (engl. *difference*).

Literatura

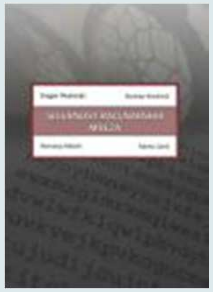
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

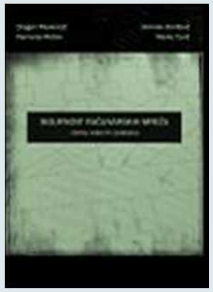
- Za predavanje 2:
  - Poglavlje 2: Sigurnosne arhitekture i modeli
  - Dodatak A: Sigurnosni standardi i programi sertifikacije

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

- Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?