Posrednici umreženih sustava

Prof.dr.sc. Siniša Srbljić

Prof.dr.sc. Dalibor Vrsalović

Dr.sc. Ivan Skuliber

Dr.sc. Dejan Škvorc

Fakultet elektrotehnike i računarstva
Laboratorij za potrošaču prilagođeno računarstvo

4. Predavanje

Sigurnosni posrednički sustavi

Miroslav Popović, mr.sc.

Fakultet elektrotehnike i računarstva
Laboratorij za potrošaču prilagođeno računarstvo

Sadržaj izlaganja

- **Oblikovanje sigurnosti posredničkog sustava**
  - Namjena, svojsva sigurnosti, zahtjevi, odredbe
- **Arhitektura sigurnosti posrednika**
  - Registracija, autorizacija, autentikacija, nadzor pristupa, praćenje korištenja
- **Pokazni primjeri na projektu MidArc**
  - Komunikacijski posrednik prividne mreže
  - Posrednik nadzora pristupa uslugama

Uloga posrednika u sigurnosti

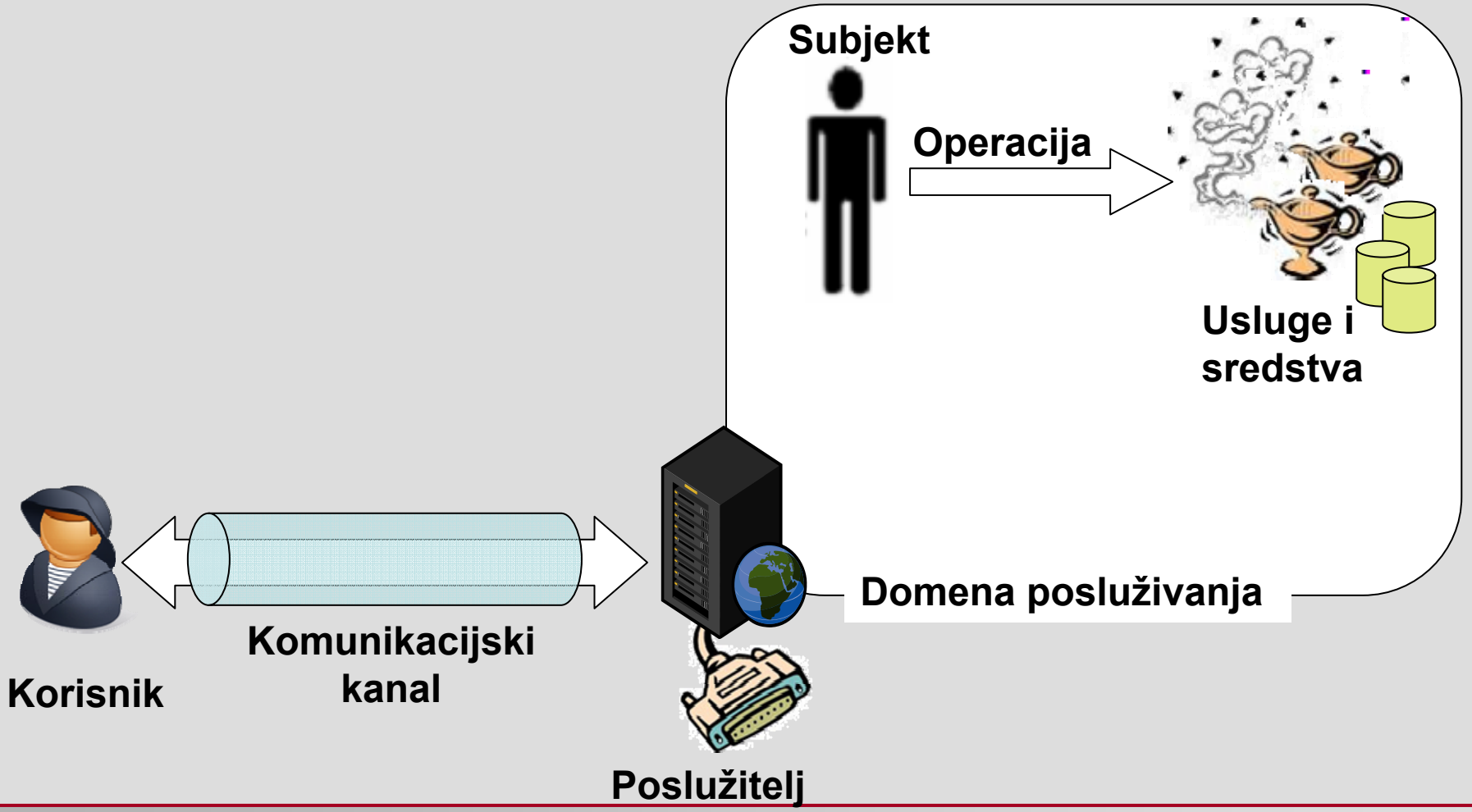
- **Sigurnost**
  - Potrebna u svakom sustavu
- **Trošak**
  - Svaki sustav gradi samostalno rješenje

- **Posrednik sigurnosti**
  - Izdvajanje sigurnosnih mehanizama u poseban sustav
  - Ponuda sigurnosti kao gotovog rješenja drugim sustavima

Očuvanje sigurnosnih svojstava

- **Sigurnosna pitanja koja treba riješiti**
  - **Tajnost ili povjerljivost** (engl. *confidentiality, secrecy*)
    - Što ako se prisluškuje?
  - **Autentičnost ili izvornost**
    - Tko je poslao zahtjev?
  - **Nepovredivost** (engl. integrity)
    - Da li korisnik smije koristiti uslugu?
  - **Pribilježenost** (engl. *accountability*)
    - Tko, kada i koliko je koristio uslugu?
  - **Neporecivost** (engl. *non-repudiation*)
    - Korisnik tvrdi da nije koristio uslugu?

Dva problema sigurnosti

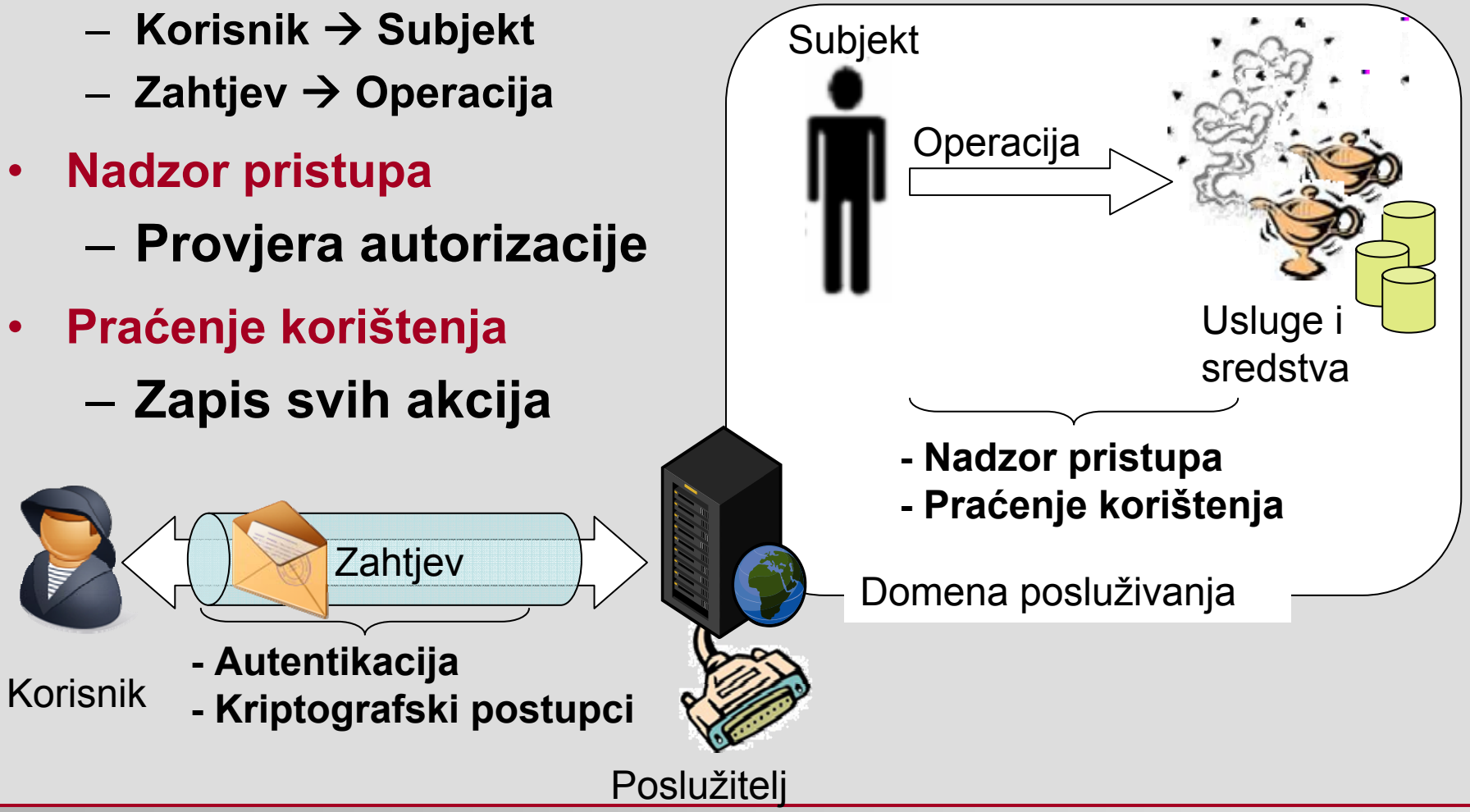


Vrste ugrožavanja sigurnosti

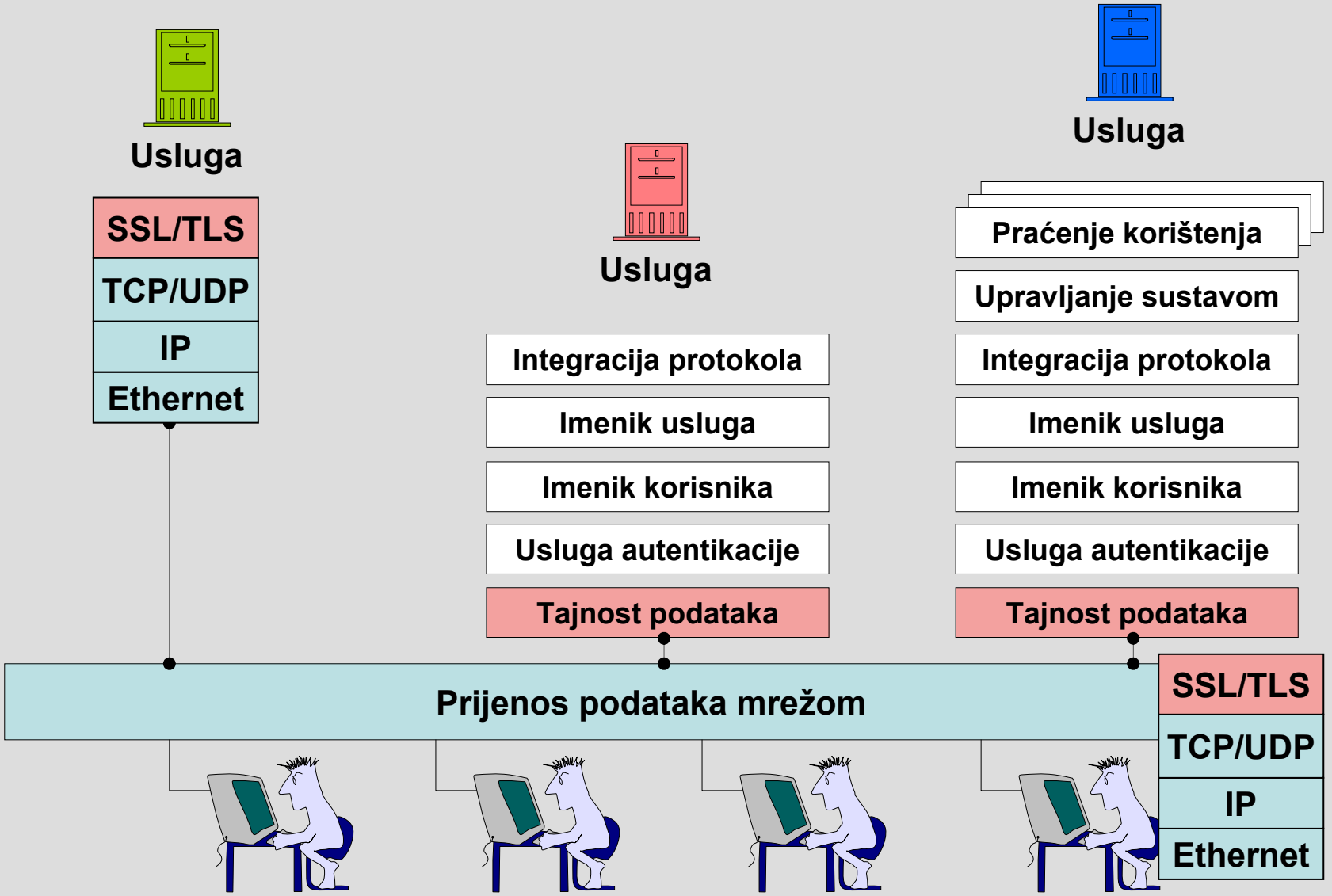
- **Prekid**
- **Prisluškivanje**
- **Izmjena**
- **Izmišljanje**

Postupci uspostave sigurnosti

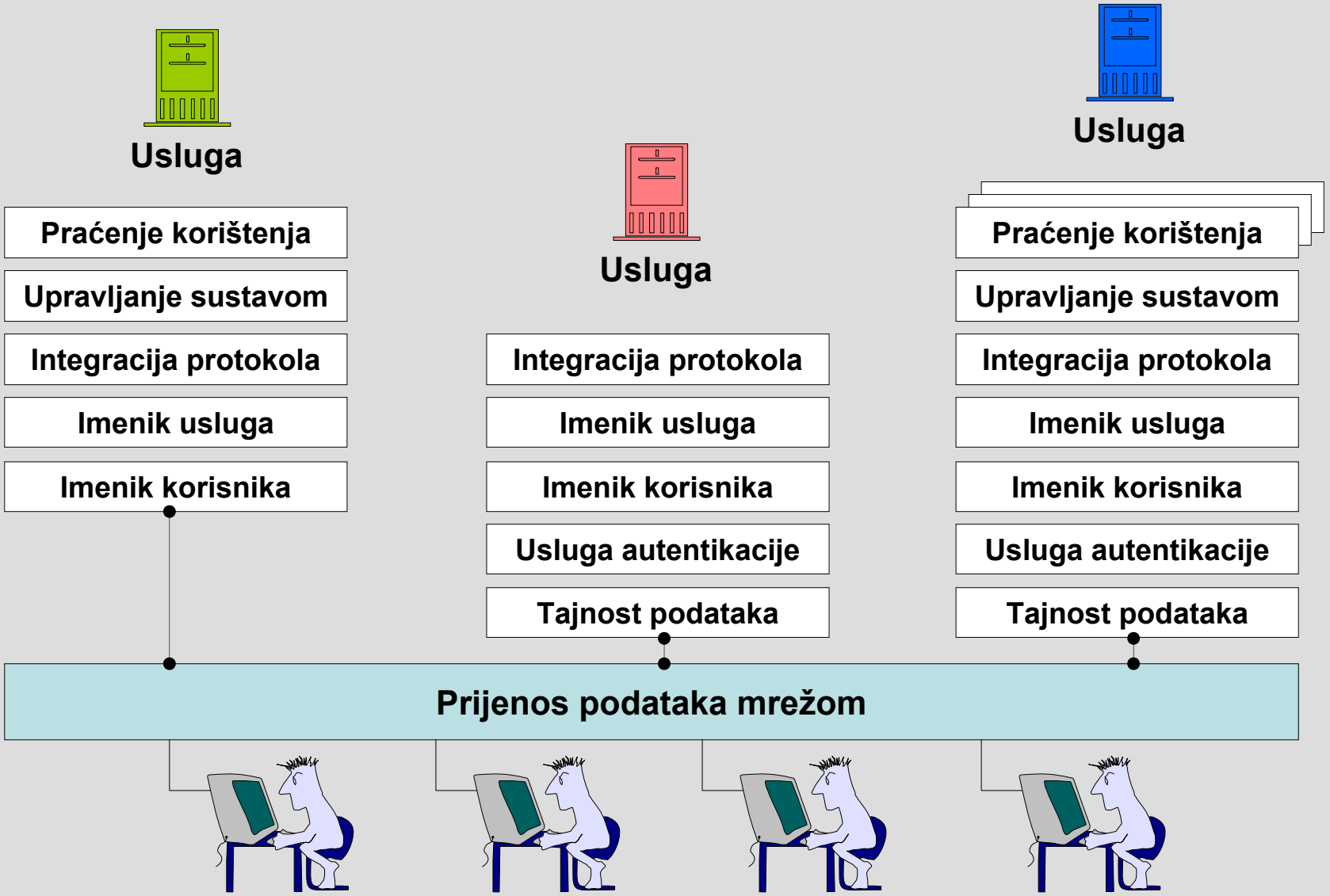
- **Autentikacija i kripto-postupci**
  - **Korisnik → Subjekt**
  - **Zahtjev → Operacija**
- **Nadzor pristupa**
  - **Provjera autorizacije**
- **Praćenje korištenja**
  - **Zapis svih akcija**



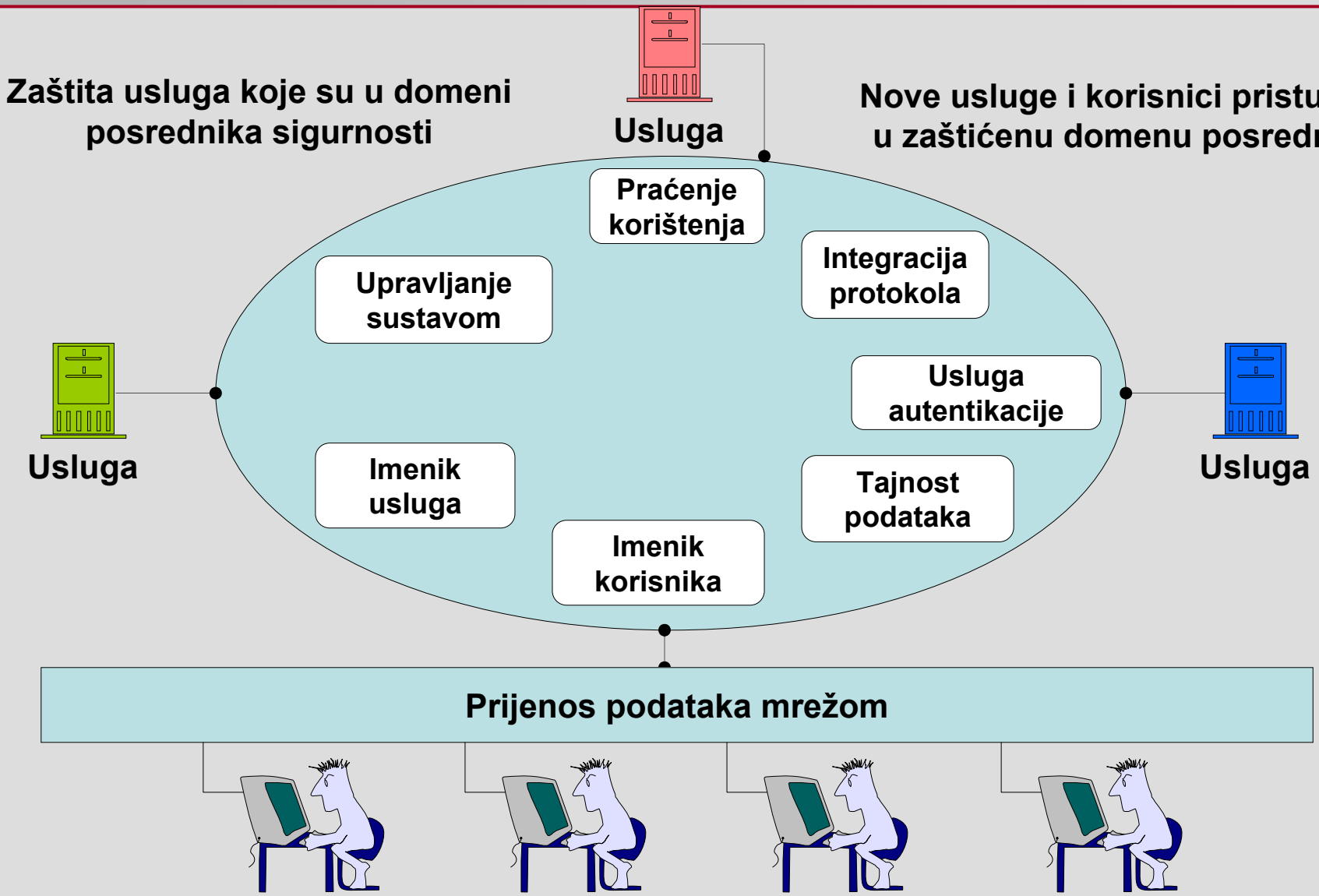
SSL posrednik sigurnosti komunikacije



Posrednik sigurnosti primjenske razine



Posrednik sigurnosti primjenske razine



Oblikovanje sigurnosti

- **Primjer odredbi sigurnosti**
  - Moguće dodavati nove usluge u sustav
  - Novi korisnici mogu ulaziti u sustav samo preko pozivnica postojećih korisnika
  - Korisnik mora biti fička osoba
  - Mora biti identificiran jedinstvenim mat.br.
  - Mora koristiti svoje pravo ime
  - Mora ostaviti telefonski broj
  - Administrator mora provjeriti korisnika telefonskim pozivom

Oblikovanje sigurnosti

- **Primjer odredbi sigurnosti**
  - Računala koja čuvaju kritične podatke moraju biti odspojena s mreže (podaci se prenose na disku)
  - Koliko često se radi backup podataka
  - Na koji medij se radi backup podataka
  - Koliko pogrešnih pokušaja prijave se dopušta
  - Što kada se detektira pokušaj provale
  - U slučaju pada servera, koga obavijestiti, koji je alternativni server

Odredbe sigurnosti

- **Analizira se**
  - Otvorenost sustava
  - Predviđeni način rada
  - Preuzimanje obaveze zaštite podataka
  - Potencijalni napadi i rizici
  - Kritične točke sustava
  - Akcije za nepredviđeni način rada i moguće napade
- **Definira se**
  - Strategija zaštite
  - Odredbe pristupa sustavu
  - Odredbe praćenja korištenja sustava
  - Odredbe prava uporabe sustava
  - Mehanizme za uspostavu odredbi sigurnosti

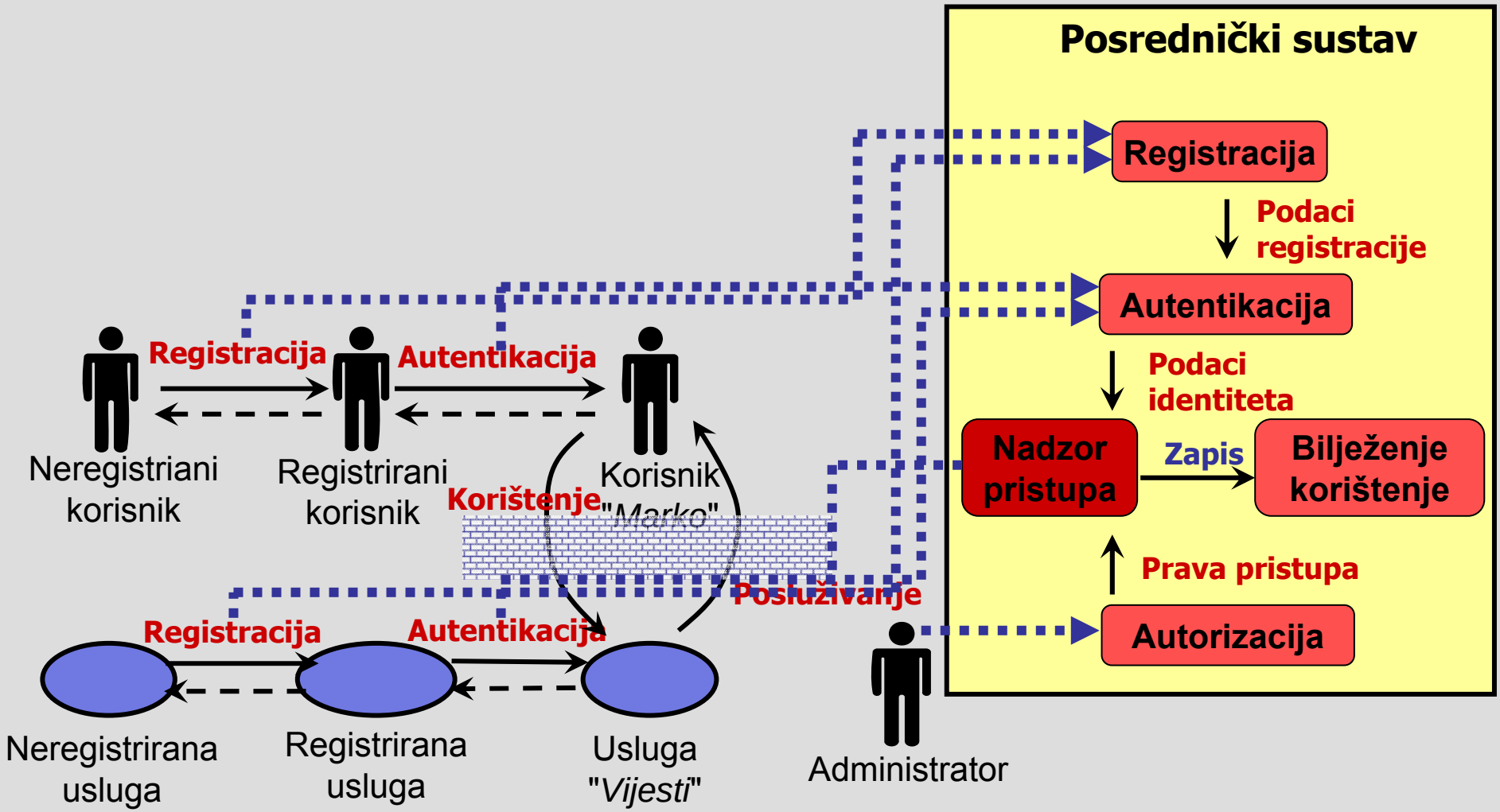
Strategija zaštite

- **Izolacija**
  - Izvan dosega bilo koga izvana Keep everybody out
- **Isključivanje**
  - Isključiti zlonamjerne korisnike
- **Ograničavanje**
  - Pustiti zlonamjerne korisnike u sustav, ali im ne dopustiti da naštete
- **Oporaviti**
  - Popraviti štetu
- **Kazniti**
  - Uhvatiti zlonamjerne počinitelje i pravno ih goniti

Mehanizmi uspostave sigurnosnih odredbi

- **Odredbe pristupa sustavu**
  - Registracija
  - Autentikacija
- **Odredbe prava uporabe sustava**
  - Nadzor pristupa
- **Odredbe praćenja korištenja sustava**
  - Bilježenje korištenja

Arhitektura sigurnosti posredničkog sustava



Registracija

- **Namjena**
  - Prikupljanje podataka o korisniku i uslugama
  - Puni imenik korisnika i usluga
  - Podaci se koriste za autentikaciju
- **Odredbe o prikupljanju podataka**
  - Zahtjeva li se identitet fizičke osobe
  - Može li se pravna osoba registrirati
  - Ista osoba više puta
  - Da li se provjerava ispravnost osobnih podataka
  - Koja vrsta autentikacijskih podataka

Registracija

- **Provjera istinitosti i-ili ispravnosti podataka**
  - Administrator
    - npr. telefonskim pozivom
  - Elektronski koristeći drugi sustav
    - npr, provjera valjanog emaila, dohvat JMBG-a u MUP-u
- **Vrste potvrde registracije**
  - Osobno podizanje potvrde
    - Poziv na telefon, zahtjevanje fizičkog dolaska, slanje faksom
  - Potvrda preko postojećeg sustava
    - Slanje podataka na e-mail

Autentikacija

- **Namjena**
  - Provjera identiteta korisnika
  - Na osnovi usporedbe podataka koji su priloženi tijekom registracije
  - Uspostava sjednice koja identificira daljni rad korisnika u sustavu
- **Vrste autentikacije**
  - Korisničko ime i zaporka (problem jedinstvenosti za različite sustave)
  - Korisnička značka (engl. token)
  - Certifikati

Autentikacija zaporkom

- **Idealna zaporka**
  - Teška za probiti, laka za pamćenje
- **Tri savjeta za odabir zaporke**
  - Randomizirane zaporke
    - Zaporka se sastoji od random znakova koji nisu poredani smisleno
  - Odredbe za kontrolu zaporki
    - Zaporke su definirane pravilima
    - Npr: zaporka mora imati najmanje 8 znakova, mora imati najmanje dva ne-slova, mora se mijenjati svakih 30 dana (*myPassword01, myPassword02, myPassword03, …* !?)
  - Zaporke sa skraćenim frazama
    - Skraćenice sastavljene od prvih slova riječi u nekoj smislenoj frazi Npr:
    - “My sister Peg is 24 years old” $\Rightarrow$ MsPi24yo

Problemi autentikacije zaporkom

- Provaljivanje zaporki
  - Napadi iz riječnika
    - Koristi riječi iz riječnika kao moguće zaporke
  - Permutacija riječi i brojeva
    - Permutira se riječi iz riječnika s brojevima
    - Zamjenjuju se uobičajeni parovi: 1 za l, 5 za S
  - Iskorištavanje korisničkih informacija
    - Poznavanje korisničkih podataka
    - Ime, prezime, ime žene, ime djece
  - Napad grubom silom

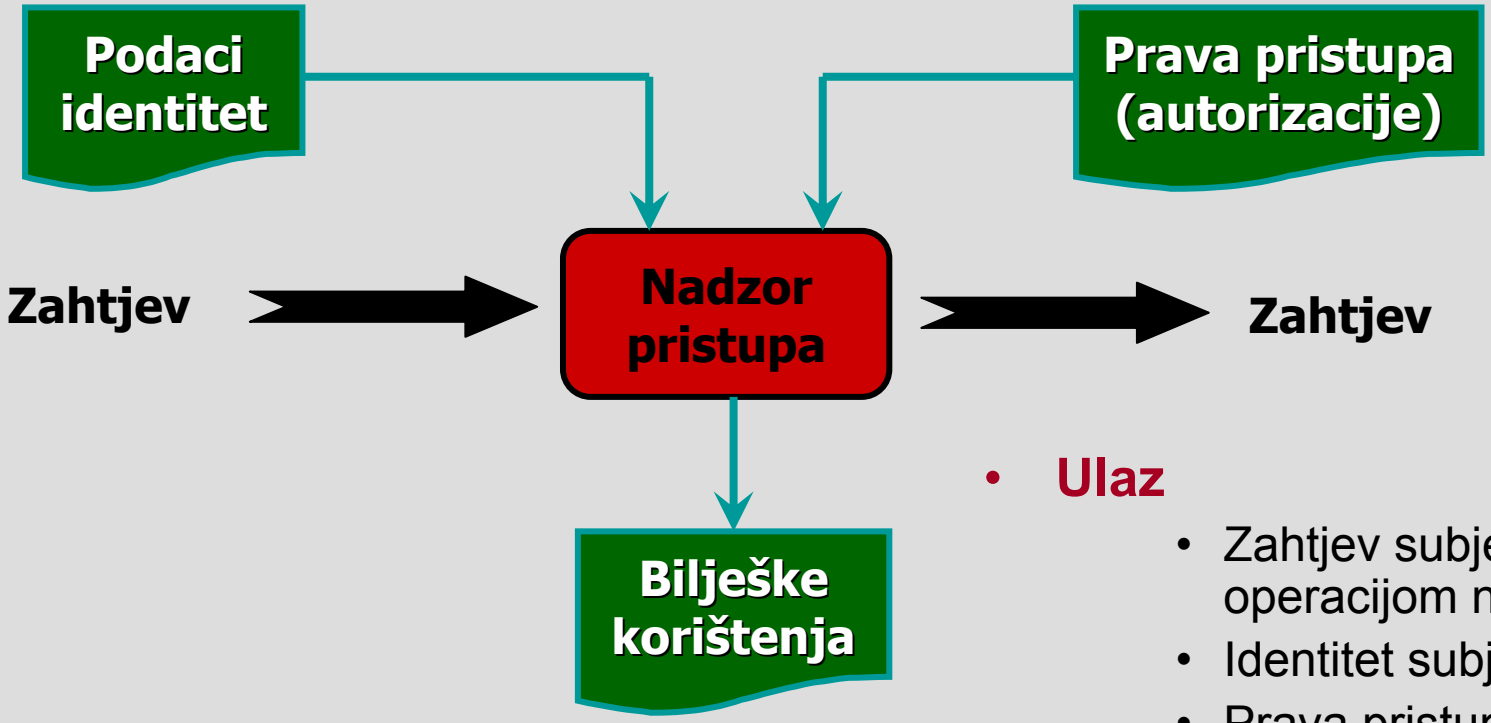
Rezultati eksperimenta provaljevanja zaporki korištenjem prve tri vrste napada

ISPITNA GRUPA	BROJ PROVALJENIH ZAPORKI
Kontrolirane zaporke	30
Randomizirane zaporke	8
Zaporke sa skraćenicama	6
Nesavjetovani korisnici	33

Nadzor pristupa

- **Namjena**
  - omogućiti ovlašten pristup sredstvima
  - spriječiti neovlašten pristup sredstvima
- **Subjekt**
  - Korisnik koji šalje zahtjev
- **Objekt**
  - Sredstvo u sustavu koje se koristi
- **Akcija**
  - Operacija nad sredstvom koju izvodi subjekt

Nadzor pristupa



- **Ulaz**
  - Zahtjev subjekata za operacijom nad objektom
  - Identitet subjekta
  - Prava pristupa
- **Izlaz**
  - Odluka o pristupu
  - Bilješka korištenja

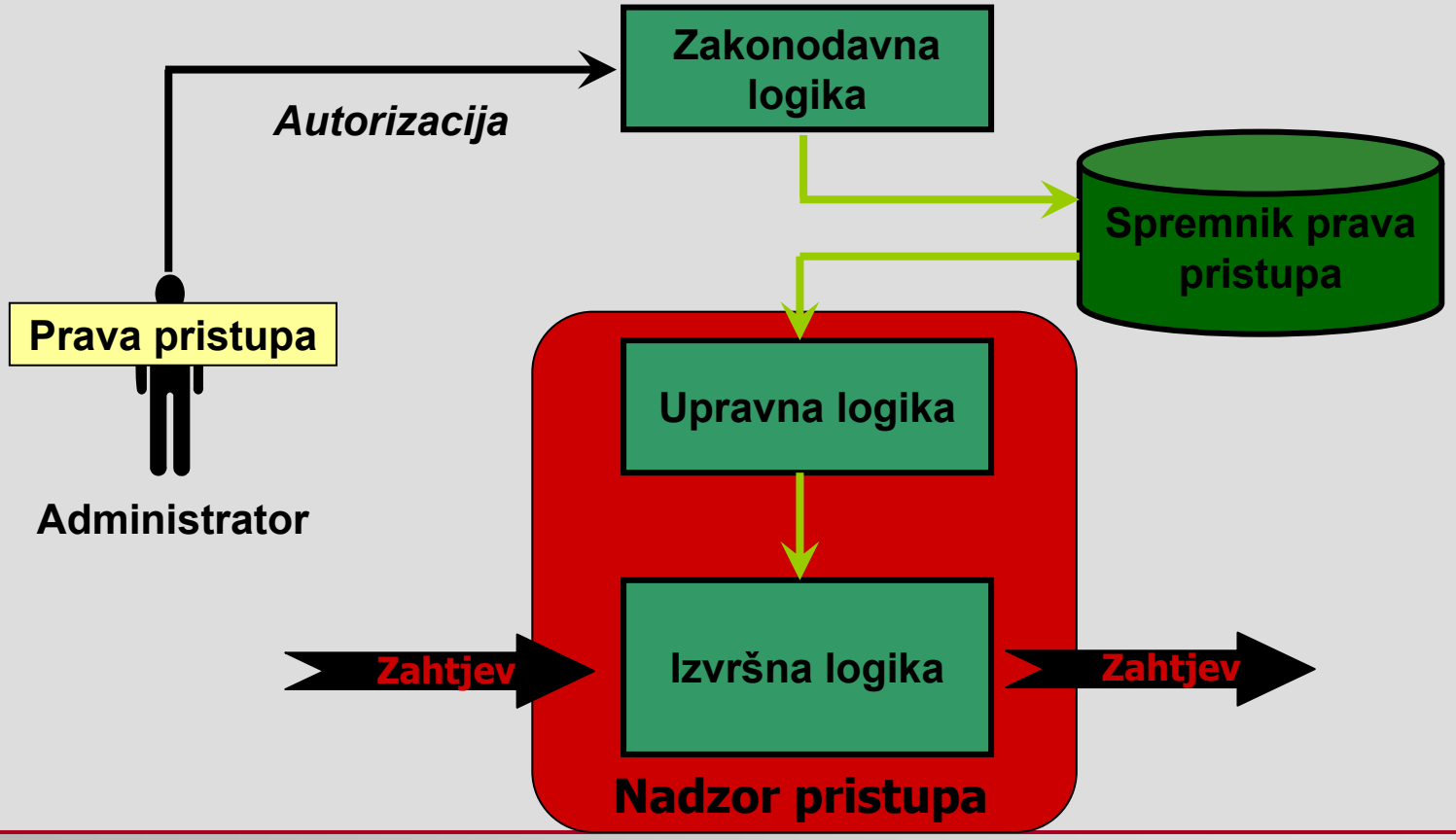
Nadzor pristupa

- **Matrica prava pristupa (engl. *access control matrix*)**
  - Osnovni model za opis prava pristupa
  - Propusnice
    - Retci matrice
    - Subjektova ovlaštenja
  - Liste pristupa, ACL (engl. access control list)
    - Stupci matrice
    - Popis korisnika koji imaju određena prava pristupa objektu.

	Sredstvo1	**Sredstvo2**	**…**	**SredstvoN**
Korisnik1	**GET, POST, PUT, DEL**	**-**	**…**	**GET**
Korisnik2	**-**	**GET, POST, PUT, DEL**	**…**	**-**
…	**…**	**…**	**…**	**…**
KorisnikM	**GET**	**-**	**…**	**GET**

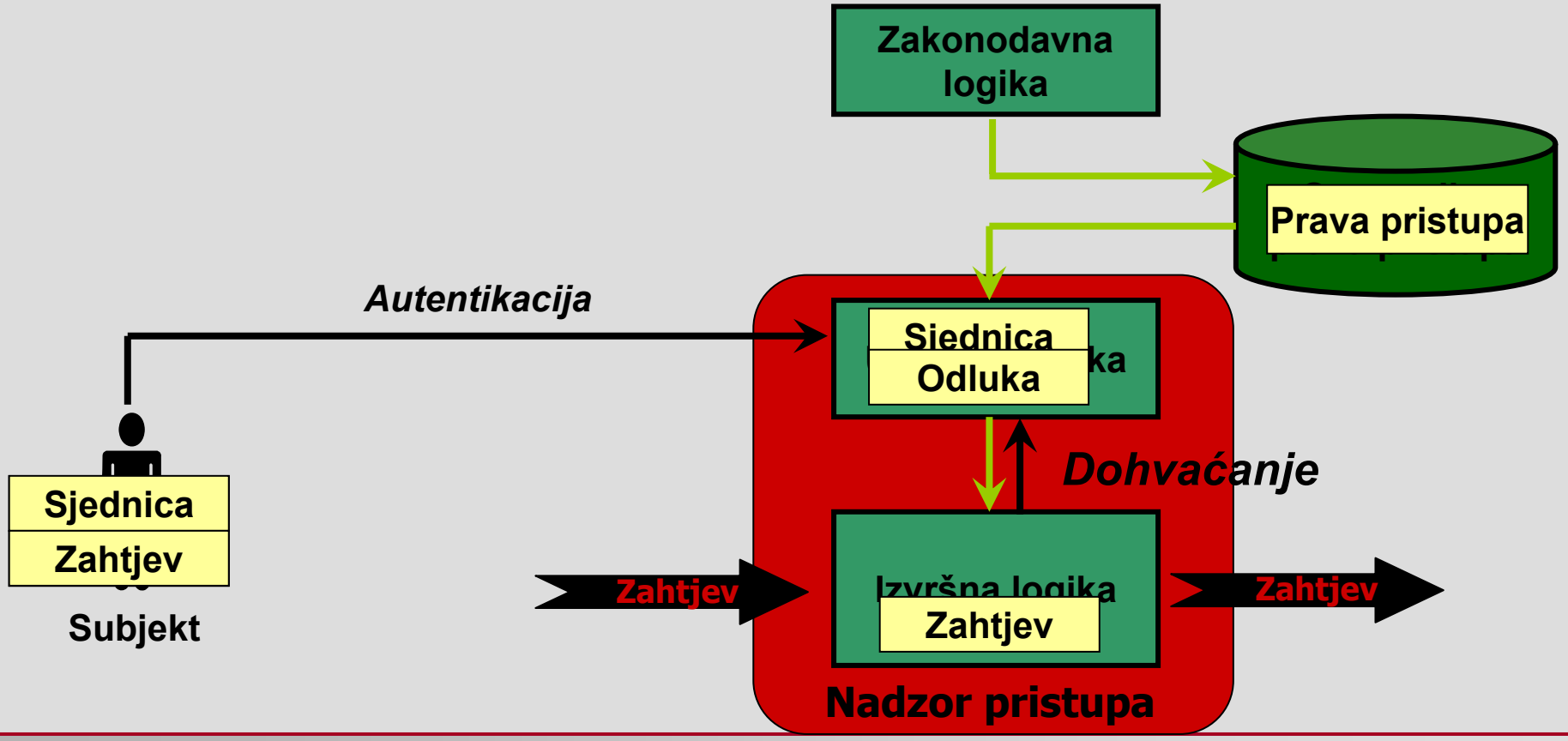
Radno okruženje nadzora pristupa

- **Razmjena podataka za nadzor pristupa**



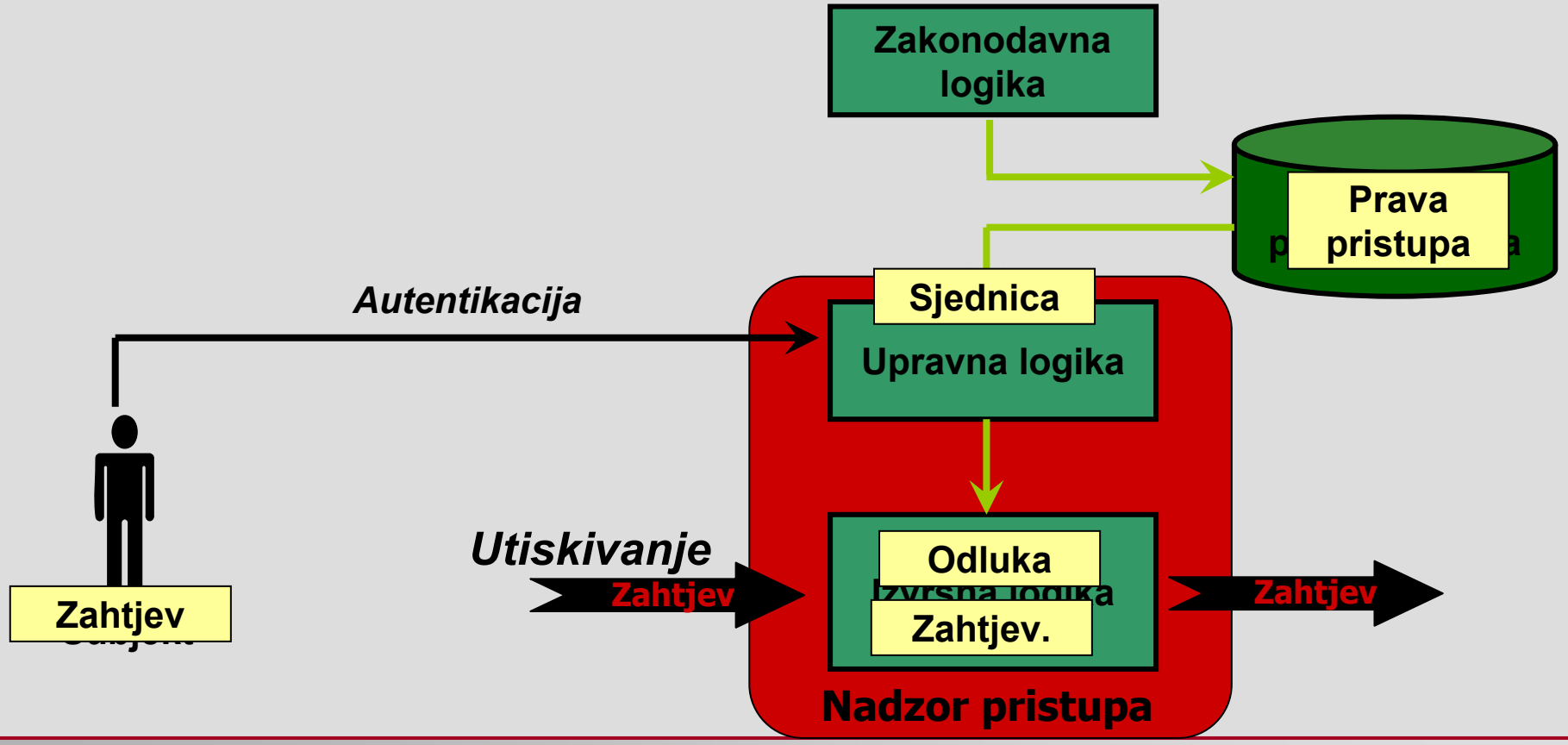
Radno okruženje nadzora pristupa

- **Razmjena podataka za nadzor pristupa**
  - Scenarij dohvaćanja prava pristupa



Radno okruženje nadzora pristupa

- **Razmjena podataka za nadzor pristupa**
  - Scenarij utiskivanja prava pristupa



Modeli nadzora pristupa

- **DAC (engl. *Discretionary Access Control*)**
  - Razlikuju se pojedinačna prava svakog subjekta
  - Prenošenje prava pristupa (engl. *delegation*)
  - Sustav za upravljanje bazom podataka
- **RBAC (engl. *Role-based Access Control*)**
  - Više korisnika objedinjuje u istu ulogu
  - Jednostavnije upravljanje korisničkim pravima pristupa
  - Web sustavi
- **MAC (engl. Mandatory Access Control)**
  - Štiti tok informacija
  - Uspoređuje razinu povjerljivosti podataka i razinu povjerenja u korisnika
  - Vojni sustavi

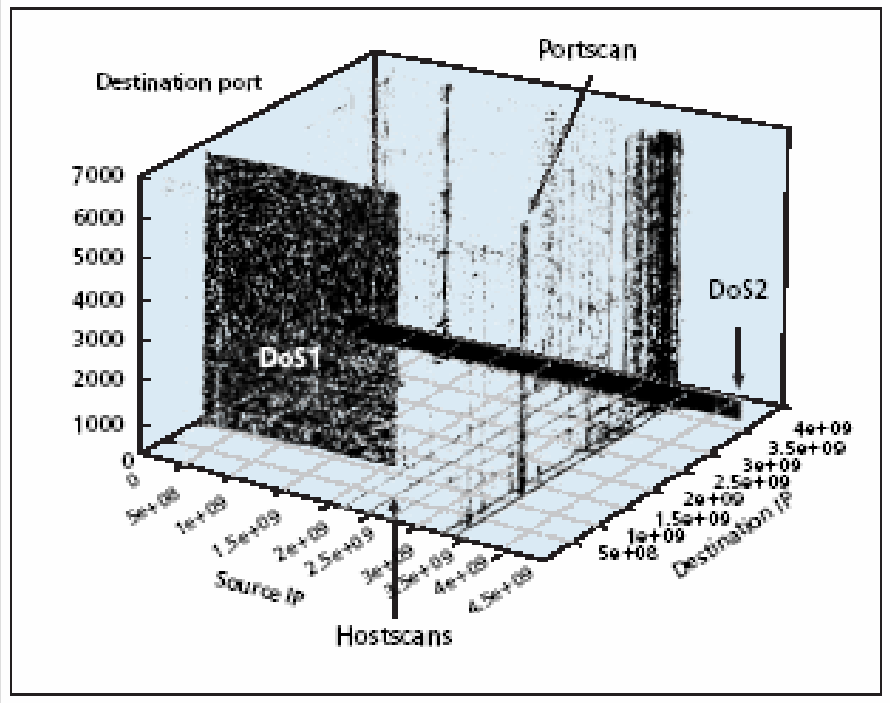
Bilježenje korištenja

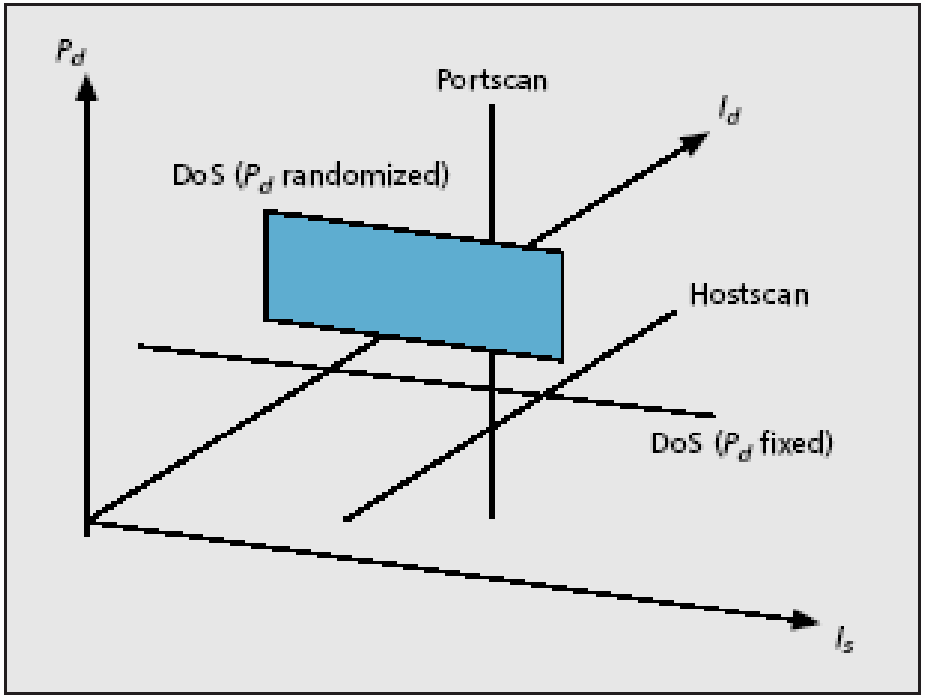
- **Kada pribilježiti korištenje**
  - svakog korisnika
  - samo određene korisnike
  - samo određene akcije
- **Što sve pribilježiti**
  - Cijeli zahtjev
  - Podatke iz tijela zahtjeva
  - Podatke iz zaglavlja zahtjeva
  - Vrijeme dolaska
  - Druge parametre sustava

Bilježenje korištenja

- **Tehnika zaštite bilježenjem korištenja**
  - Prepoznavanje napada DoS (engl. *denial of service*) u realnom vremenu
  - 3D vizualizacija mrežnog prometa

flow = ƒ(sourceIP, destinationIP, destinationPort)





Bilježenje korištenja

- **Personalizacija**
  - Korisnici perosnaliziraju usluge prema svojim željama
    - Uporaba usluga na korisniku intuitivan način
    - Brže pronalaženje tražene informacije
  - Pružatelji usluga skupljaju informacije o korisniku
    - Bolja prilagodba korisničkom profilu
    - Nude nove usluge, produkte i informacije ciljane prema korisniku
- **Izgradnja korisničkih profila**
  - Implicitno rangiranje
    - Ne upadljiva metoda, ne prekida korisnika u radu
    - Pribilježava korisničke akcije u pozadini
  - Eksplicitno rangiranje
    - Nije u okviru bilježenja korištenja
    - Traži eksplicitnu povratnu informaciju of korisnika

Personalizacija

- **Problemi privatnosti**
  - Sakupljeni podaci mogu se iskoristiti u zlonamjerne i u dobronamjerne svrhe
  - Korisnikova privatnost je narušena ako se njihov korisnički profil proda drugim kompanijama
  - Problemi predstavlja prikupljanje korisničkih informacija bez korisnikovog znanja i eksplicitne dozvole
  - Korisnici će cijeniti personalizaciju ako im se ponudi zanimljiva usluga, produkt ili informacija

Pokazni primjer

- **Suradnja FER/ZEMRIS i tvrtke Ericsson Nikola Tesla**
  - MidArc posrednik
- **Ciljevi MidArc posrednika**
  - Sustav za potporu rada prividnih organizacija
  - Posrednički sustav zajedničkih funkcionalnosti korištenja usluga
  - Sigurno, pouzdano i naplativo korištenje usluga
- **Primjeri**
  - Komunikacijski posrednik prividne mreže
  - Posrednik nadzora pristupa uslugama

Komunikacijski posrednik prividne mreže

Prividna komunikacijska mreža

- Komunikacija zasnovana na porukama
  - SOAP poruke zasnovane na XML-u
- Topologija i prosljeđivanje na primjenskoj razini
- Logički prostor adresiranja nezavisan od DNS

Sigurnost komunikacije u prividnoj mreži

- WS-Security

Zahtjevi sigurnosti	Tehnologije
Autentikacija	**X.509 digitalni certifikati**
Tajnost	**XML Encryption**
Nepovredivost	**XML Digital Signature**
Autorizacija	**Access Control Liste**

Komunikacijski posrednik prividne mreže


```
<soap:Envelope>
    <soap:Header>
        <From>Node_A</From>
        <To>Node_D</To>
        <Rev>Node_A</Rev>
        <Fwd>Node_B</Fwd>
    </soap:Header>
     <soap:Body>
        <UpdateBankAccount>
            <number>657-34-584</number>
            <amount>1000</amount>
        < UpdateBankAccount >
    </soap:Body>
</soap:Envelope>
```

Komunikacijski posrednik prividne mreže


```
<soap:Envelope>
    <soap:Header>
        <From>Node_A</From>
        <To>Node_D</To>
        <Rev>Node_A</Rev>
        <Fwd>Node_B</Fwd>
    </soap:Header>
     <soap:Body>
        <UpdateBankAccount>
            <number>657-34-584</number>
            <amount>1000</amount>
        < UpdateBankAccount >
    </soap:Body>
</soap:Envelope>
```

Komunikacijski posrednik prividne mreže


```
<soap:Envelope>
    <soap:Header>
        <From>Node_A</From>
        <To>Node_D</To>
        <Rev>Node_B</Rev>
        <Fwd>Node_C</Fwd>
    </soap:Header>
     <soap:Body>
        <UpdateBankAccount>
            <number>657-34-584</number>
            <amount>1000</amount>
        < UpdateBankAccount >
    </soap:Body>
</soap:Envelope>
```

Komunikacijski posrednik prividne mreže


```
<soap:Envelope>
    <soap:Header>
        <From>Node_A</From>
        <To>Node_D</To>
        <Rev>Node_C</Rev>
        <Fwd>Node_D</Fwd>
    </soap:Header>
     <soap:Body>
        <UpdateBankAccount>
            <number>657-34-584</number>
            <amount>1000</amount>
        < UpdateBankAccount >
    </soap:Body>
</soap:Envelope>
```

Komunikacijski posrednik prividne mreže

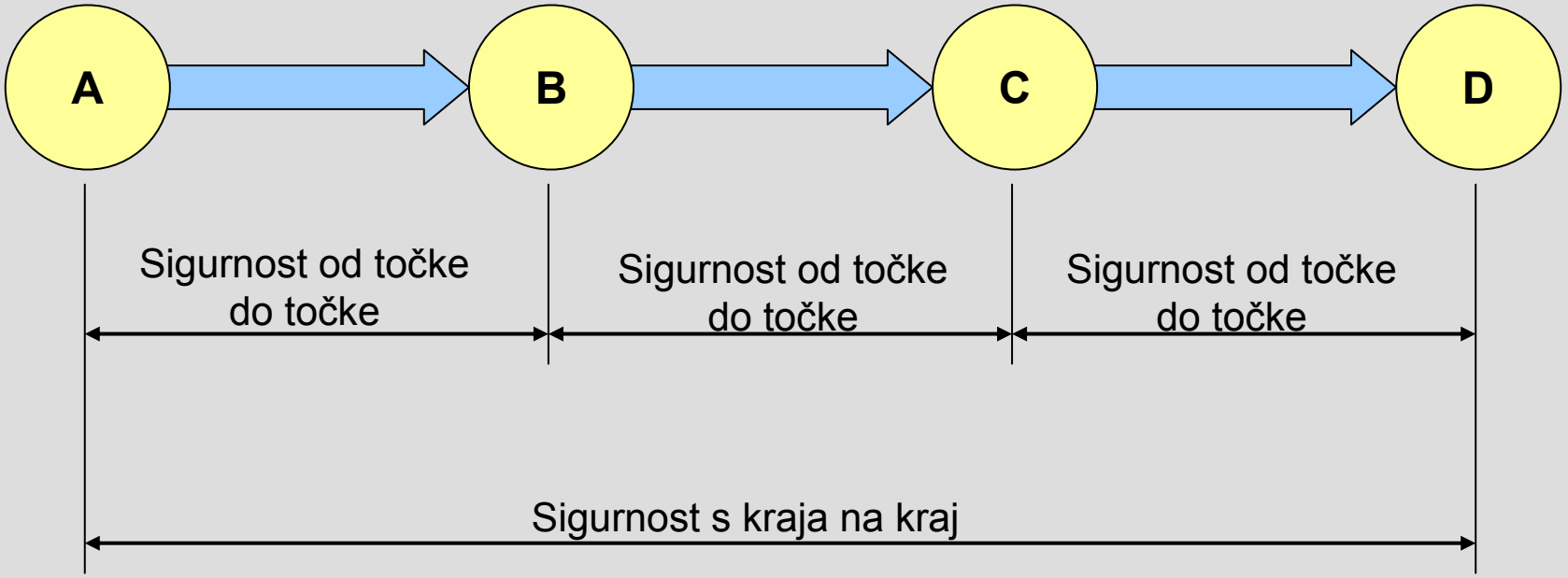

```
<soap:Envelope>
    <soap:Header>
        <From>Node_A</From>
        <To>Node_D</To>
        <Rev>Node_C</Rev>
        <Fwd>Node_D</Fwd>
    </soap:Header>
     <soap:Body>
        <UpdateBankAccount>
            <number>657-34-584</number>
            <amount>1000</amount>
        < UpdateBankAccount >
    </soap:Body>
</soap:Envelope>
```

Potpisao A

Potpisao C

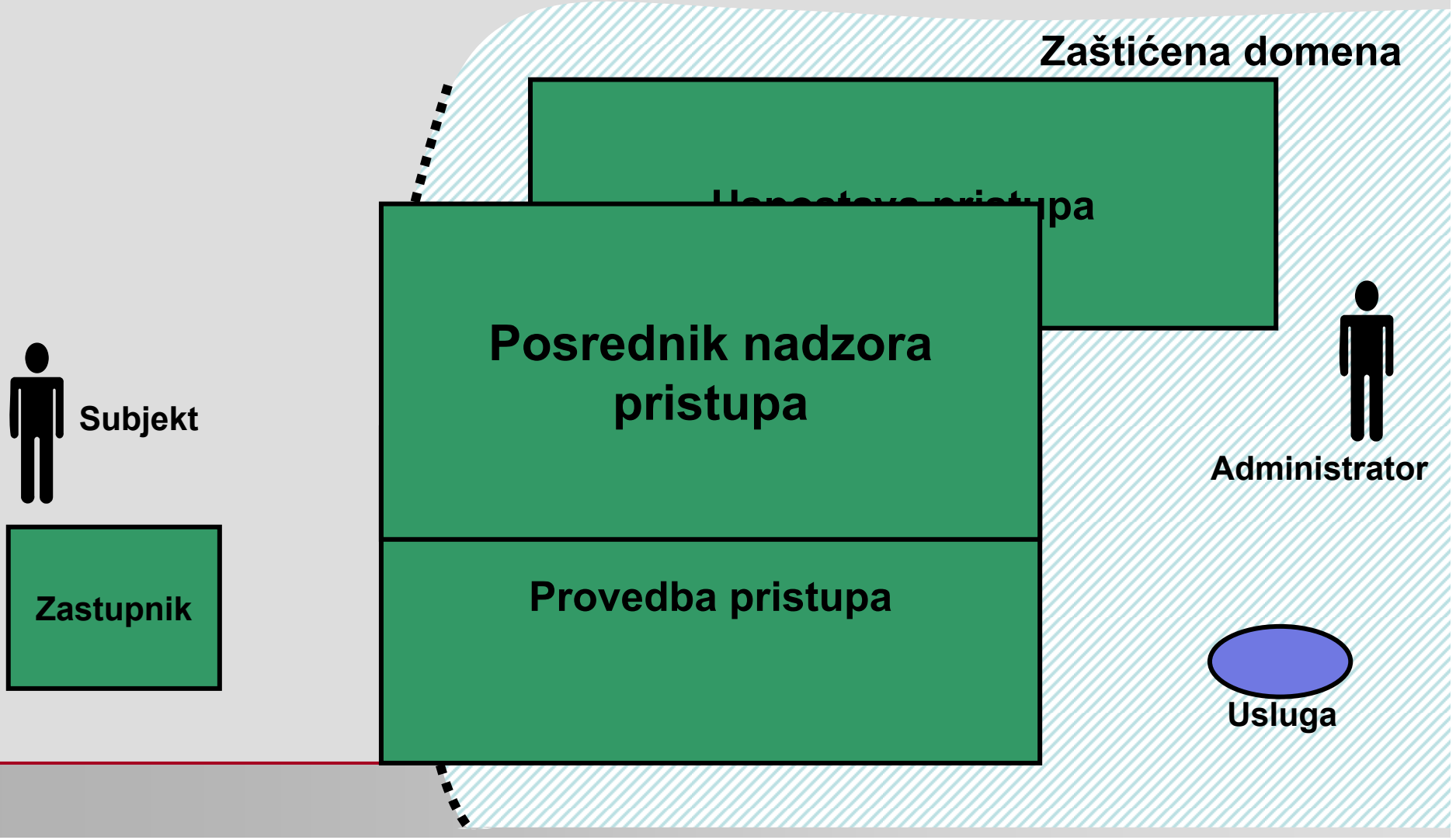
Kriptirano za D
+
Potpisao A

Komunikacijski posrednik prividne mreže



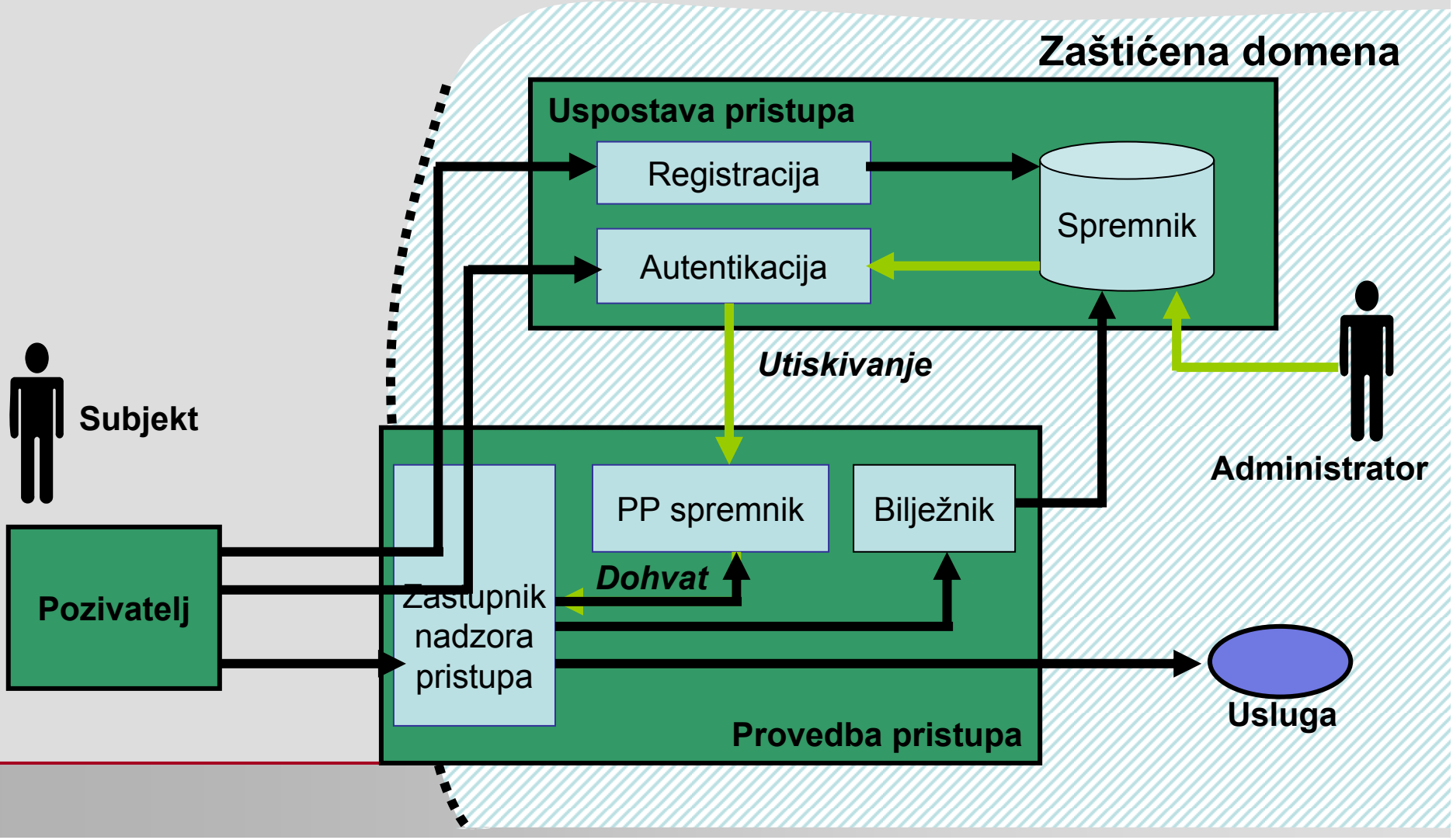
Posrednik nadzora pristupa uslugama

- **Globalna arhitektura**



Posrednik nadzora pristupa uslugama

- **Globalna arhitektura**



Literatura

- Dejan Škvorc, “Sigurni prijenos podataka u mrežama s posredničkim sustavima”, diplomski rad, Zagreb, 2003.
- Miroslav Popović, “Nadziranje pristupa računalnim sustavima zasnovanim na uslugama”, magistarski rad, Zagreb, 2006.
- Tomislav Čohar, “Sigurnosni mehanizmi u logičkim komunikacijskim mrežama s ravnopravnim sudionicima”, diplomski rad, Zagreb, 2005.