Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

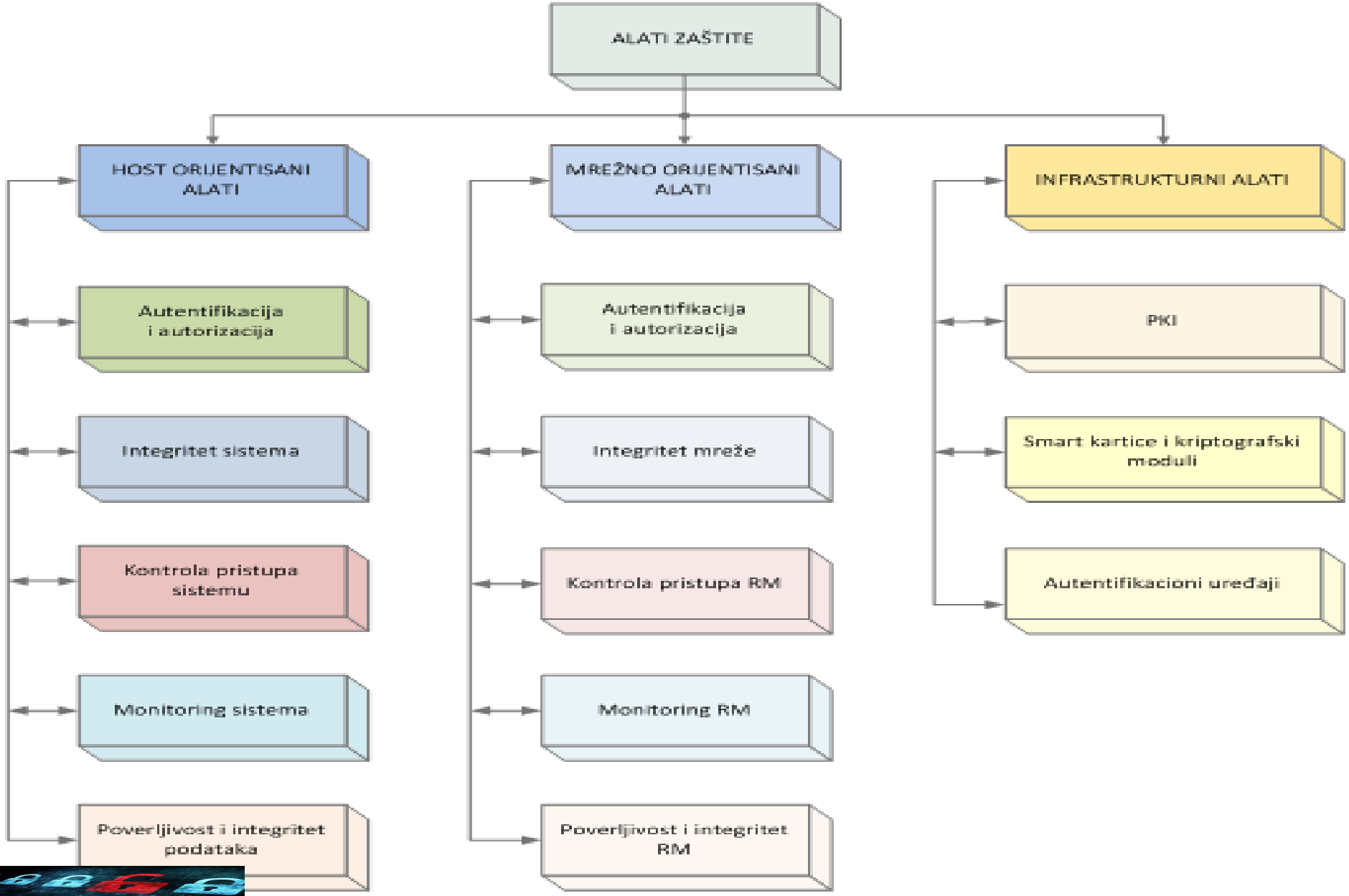
8. TEHNOLOGIJE ZAŠTITE RAČUNARSKE MREŽE

CILJ

Razumeti i naučiti:

- osnovne **razlike i sličnosti** tehnologija zaštite RS i RM
- **osnovne alate** (mehanizme i protokole) za zaštitu RM
- **infrastrukturne komponente** zaštite RM (PKI, smart kartice)
- **standarde, ograničenja i tehnologije** zaštite bežičnih RM

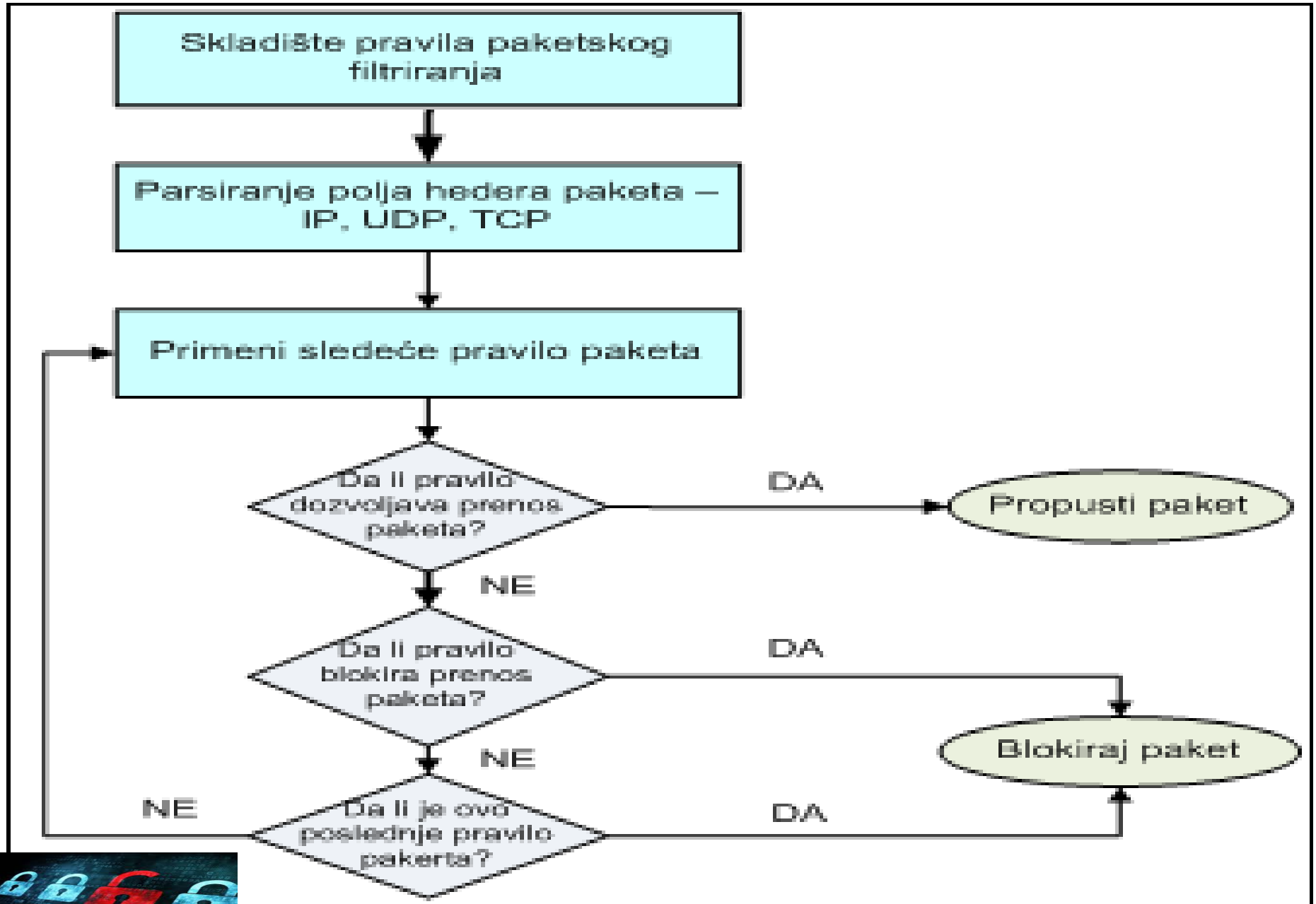
OO šema klasifikacije alata za zaštitu



Kontrola pristupa RM
-Mrežne barijere (Firewalls)-

- **Koncept LAC u RS u toj formi ne postoji u RM**
- **Za LAC između dve RM koriste se tehnike**:
  - *filtriranja paketa* u **TCP/IP** okruženju sa firewalls
  - *uspostavljanje zatvorenih grupa* u **X.25** *okruženju*
- Nameću politiku **AC** između segmenata RM
- Kontrolišu mrežni pristup dolaznog/odlaznog saobraćaja na ***mrežnom, transportnom i aplikativnom*** sloju
- **Dopuštaju/odbijaju konekcije dve RM**
- Generalno **rade na aplikativnom nivou**, ne prepoznaju protokole koji nisu TCP/IP
- Koriste ograničeni skup podataka za rad i vrše **ograničenu mrežnu zaštitu** po dubini

Primer: Procesa filtriranja paketa mrežne barijere

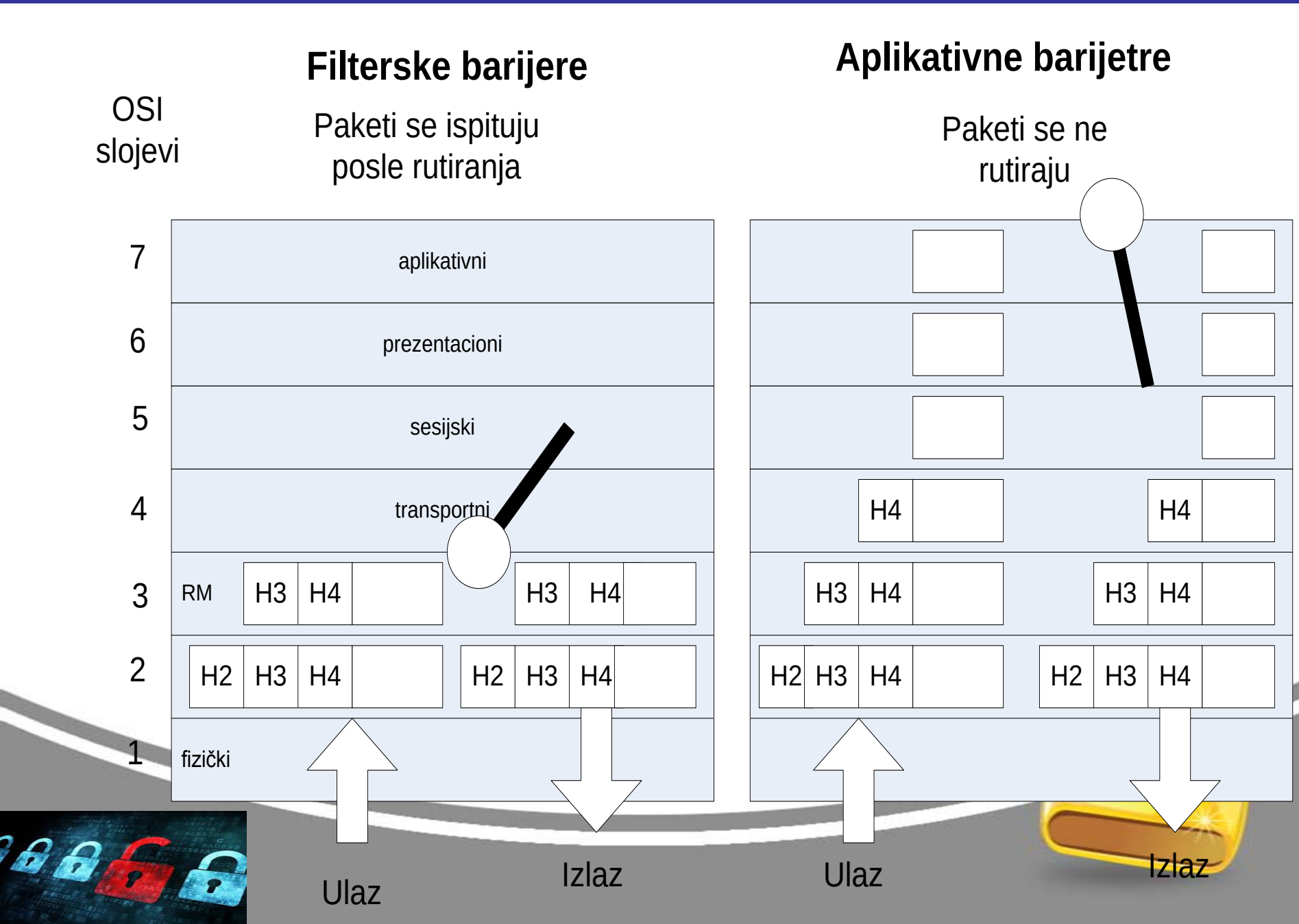


Tipovi logičkih barijera (*Firewalls*)

1. **Sa *potpunom kontrolom „stanja“ konekcija*:**
   - **filtriraju rutirane IP pakete** između interfejsa 2 i 3 sloja RM
   - **analiziraju protokole** OSI slojeva **3 – 7** i „**stanje**“ veze

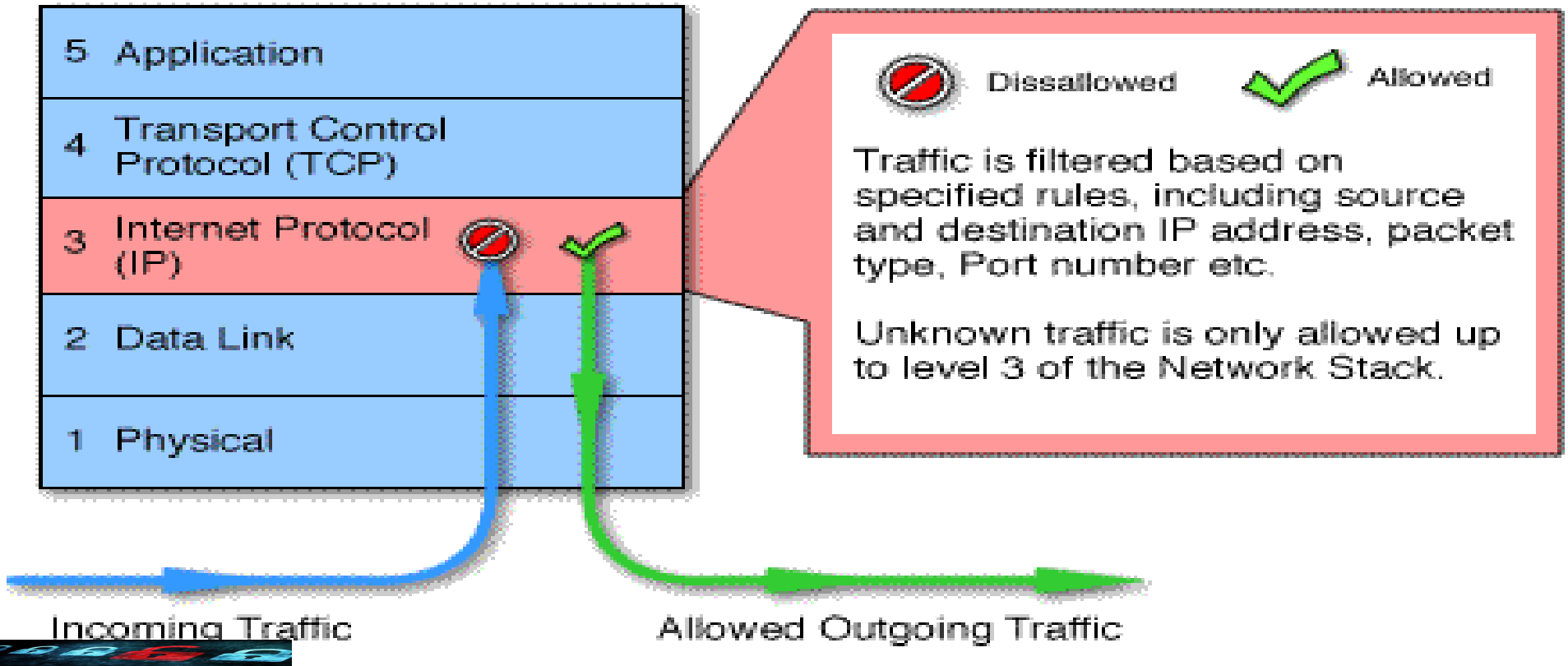
2. **Na aplikativnom sloju (*gateway*)** ili *proksi barijere*:
   - **ne rutiraju pakete** - procesiraju ih komun. programom
   - **prenose pakete aplikaciji koja analizira protokol**
   - većina savremenih protokola nemaju proksi barijere
   - koriste se za kontrolu **std.** Internet **protokola** (FTP, HTTP)
   - proizvođači **često kombinuju obe barijere**

Primer: Principi rada filterskih i aplikativnih barijera



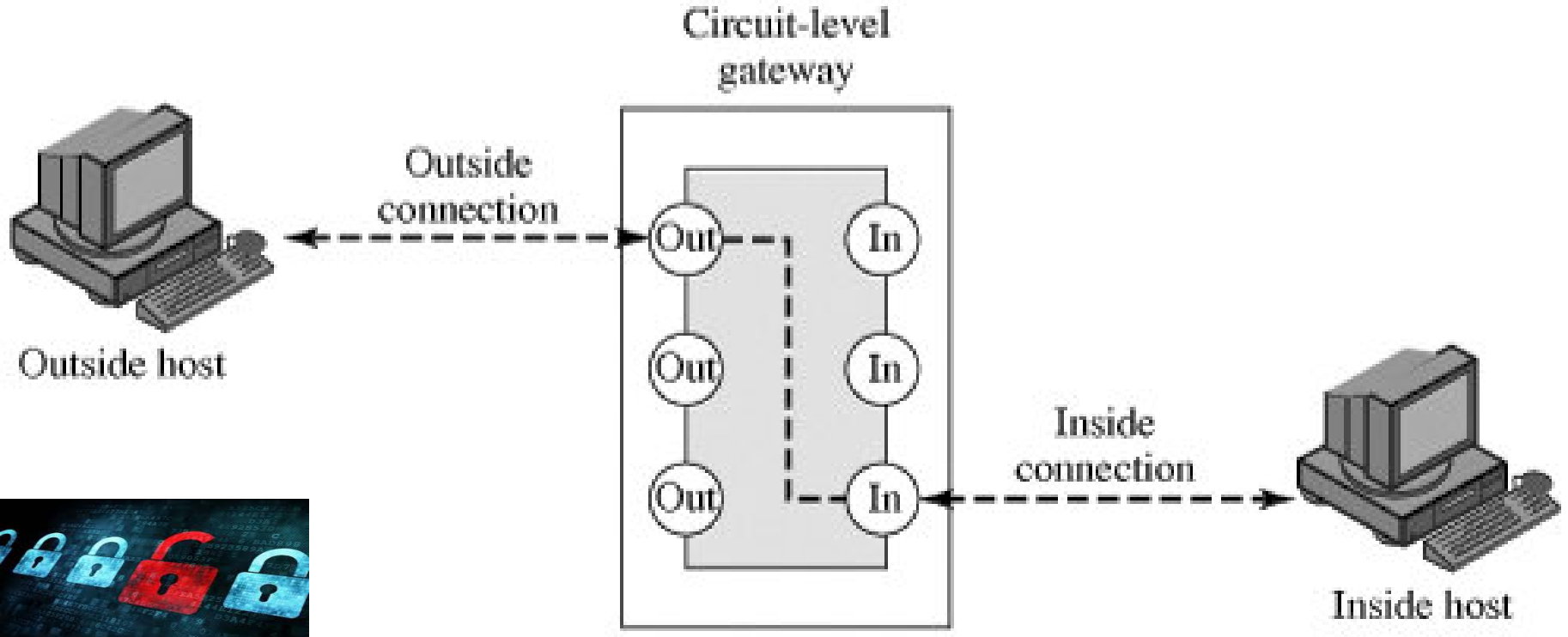
Primer: Barijera na mrežnom sloju

- Paketi se filtriraju **na bazi izvorišne, odredišne IP adrese**, **tipa paketa, broja porta** itd.
- Nepoznati saobraćaj se dopušta samo do mrežnog sloja OSI modela RM

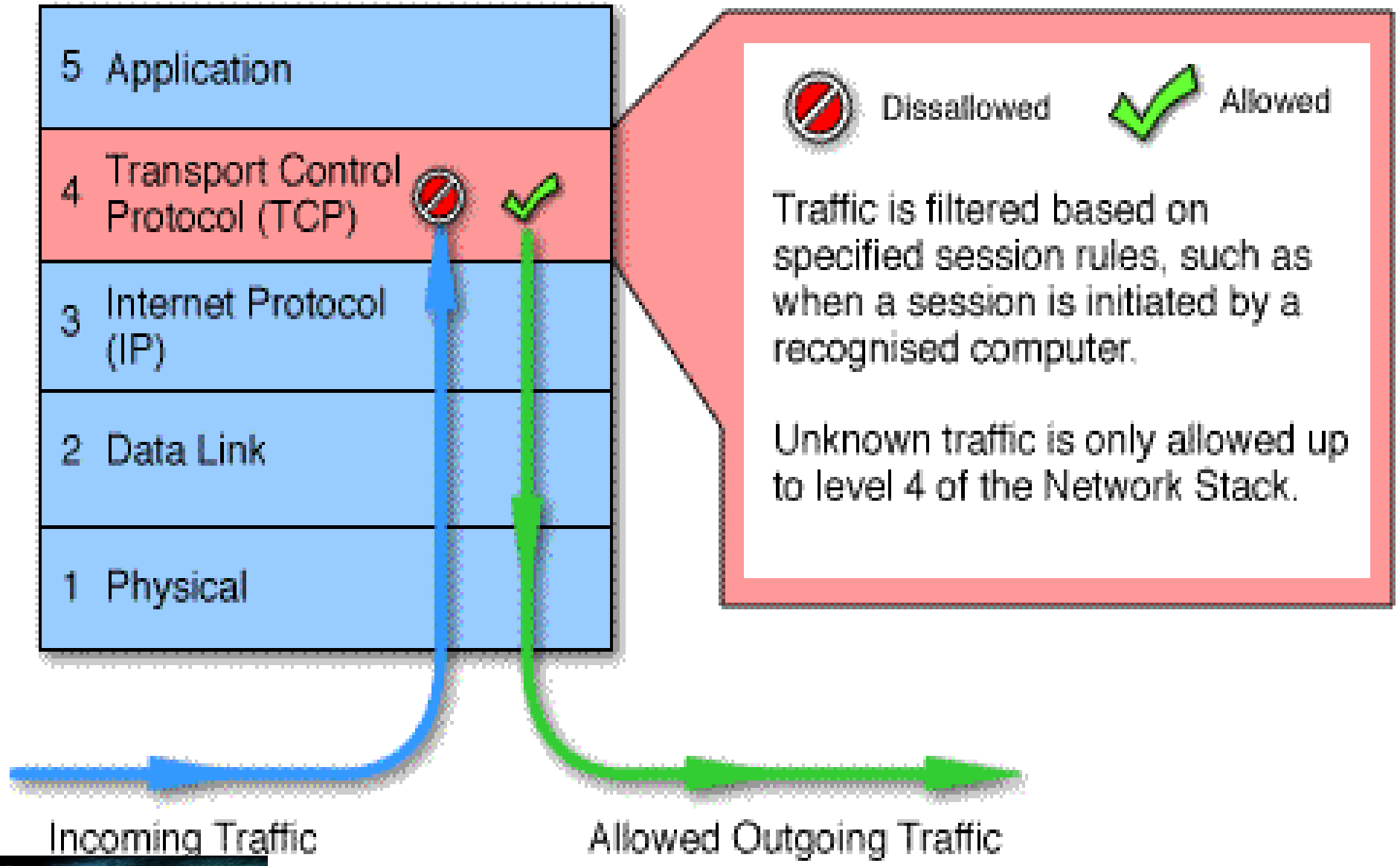


Barijera na transportnom sloju

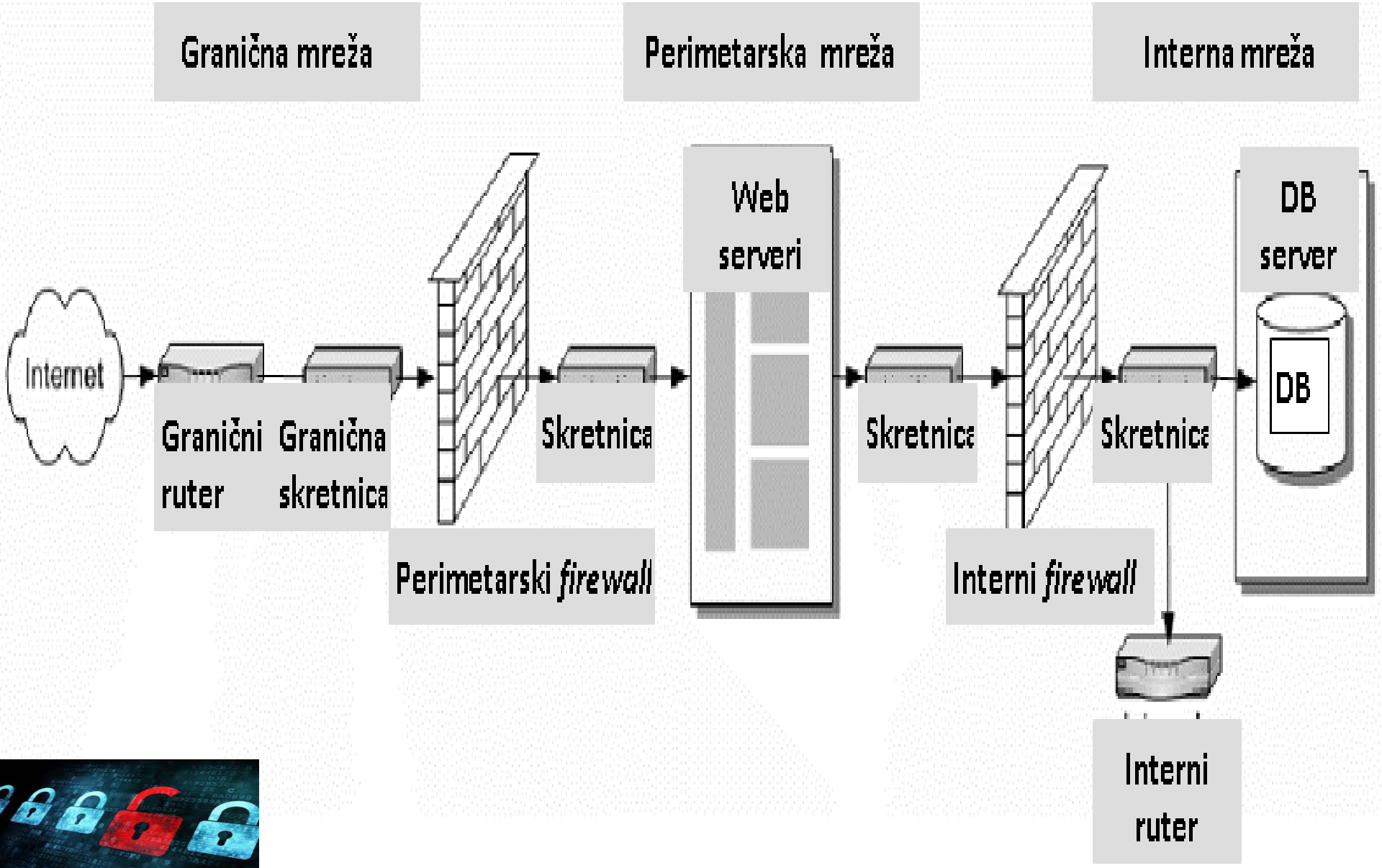
- **Ne dozvoljava TCP konekciju** sa jednog kraja na drugi
- **Uspostavlja dve TCP konekcije na bazi pravila sesije**:
  - *sa TCP korisnikom u RM i TCP korisnikom izvan RM*
- Kada se uspostave **obe konekcije**, **prosleđuje TCP segmente** bez provere sadržaja.
- Koristi se gde **administrator veruje internim korisnicima**



Primer: Barijera na transportnom sloju



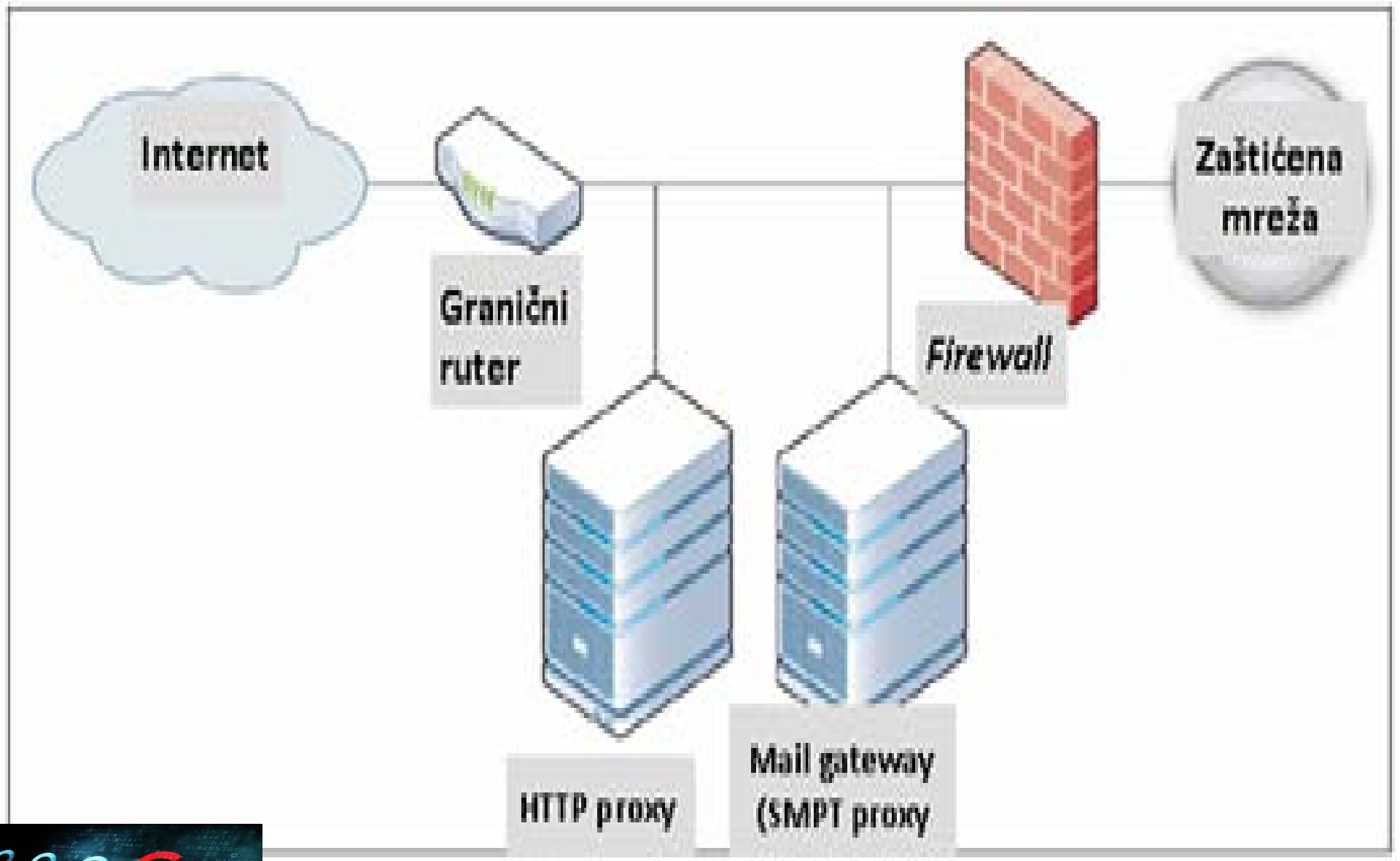
Primer: Zaštita perimetra RM sa dve barijere



Proksi serveri

- rade *slično aplikativnim gateway* barijerama
- **kontrolišu konekcije koje dolaze iz interne RM**
- **zahtevaju autentifikaciju krajnjeg korisnika**
- redukuju **AC** i veze na definisani skup protokola
- **loguju kontrolne tragove**
- **najčešći tip**: **web proksi server** samo za zaštitu
- striktno nisu mehanizmi za zaštitu RM
- pre su **višefunkcionalni mehanizmi** sa funkcijom zaštite

Primer: Konfiguracija aplikativnog proksija



Web filteri

- **Koriste se za kontrolu**:
  - *produktivnosti i pristupa internih korisnika web lokacijama*
- **Selektivno blokira pristup zabranjenim *web* lokacijama**:
  - *na bazi lokalne politike zaštite* (slično ažuriranju AVP)
- **Neki provajderi poseduju inteligentne agente:**
  - analiziraju sve posećivane *web* lokacije i ažuriraju baze podataka
- **Tipično uključuju**:
  - *blokiranje određenih kategorija sadržaja sa web lokacija*
  - *restrikcije za određeni period dana*
  - *definisanje načina monitorisanja pokušaja pristupa*
  - *izdavanje standardnih i kastomizovanih izveštaja i*
  - *praćenje ponašanja korisnika i poseta lokacijama*

Mrežna kontrola pristupa
-Autentifikacioni protokoli-

- **TCP/IP mreža: nije bezbedna** - autentifikacija pasvordom
  - zaštita infrastrukture RM deo rešenja, ali ne obuhvata neovlašćenu opremu za pristup RM (*snifer-a,* npr.)
- Ne može se verovati u tuđe mere zaštite na Internetu
- **Neophodno je ugraditi mere zaštite u proces razmene** p/i:
  - **uobičajen način - standardni autentifikacioni protokoli**
- **Protokoli zaštite -** kompleksni i teški za podele
- **Autentifikacioni protokoli - oblast za sebe**

Primer: Mrežni protokoli sa poznatim ranjivostima

Protokol	Osnovne ranjivosti
FTP	Nema kriptozaštitu, izlaže korisničko ime, lozinke i podatke u OT.
TELNET	Ranjiv na preplavljivanje bafera, povratni odgovor i *spoofing* za dobijanje privilegija i otkrivanje lozinke.
HTTP	Više ranjivosti u raznim implementacijama; slaba konfiguracija HTTP servera omogućava eskalaciju privilegija.
LDAP i MS *Directory Services*	Neke implementacije su podložne preplavljivanju bafera i DoS napadima sa mogućnošću izmene privilegija.
SNMP	Mogući DoS napadi i preplavljivanje bafera, ako ostane ime organizacije i dr. podaci u predefinisanoj konfiguraciji; može omogućiti eskalaciju privilegija i kompromitaciju.
SSH (*Secure Shell*)	Kada protokol radi pod nalogom ruta, mogući su DoS napadi, eskalacija privilegija i kompromitacija.
DNS	Više bezbednosnih ranjivosti u raznim implementacijama.

Autentifikacioni protokoli

- **Protokoli za autentifikaciju:**
  - više su vezani za korisnike i uređaje nego za podatke
  - koriste **DS** i **MAC** (*Message Authentication Codes*)

1. Vremenski sinhronizovani protokoli:

- oslanjaju se na sinhronizaciju časovnika u RM

2. Asinhroni protokoli:

- koriste protokole tipa ***upit-odgovor*** (tipa *Kerberos*)
- **nisu osetljivi na nesinhronizaciju časovnika**

Autentifikacioni protokoli - SSL

- **SSL (*Security Socket Layer*) protokol obezbeđuje**:
  - autentifikaciju **servera klijentu, klijenta serveru** i
  - uspostavu **kriptološki zaštićene komunikacije (sesije)**
- **Za dokazivanje autentičnosti** koriste:
  - ***digitalni sertifikat*** (DS), koji izdaje sertifikaciono telo – **CA**
  - **aplikacija za verifikaciju DS** proverava valjanost DS
- **Pošiljalac DP podatke, a primalac verifikuje**:
  - time se vrši **zaštita integriteta podataka ses**ije
- **Pošiljalac šifruje podatke, a primalac dešifruje**:
  - time se vrši **zaštita poverljivosti sesije**

Autentifikacioni protokoli – SSL (1)

- **SSL protokol** koristi dva podprotokola:
  1. **SSL protokol zapisa poruka** (*SSL record protocol*):
     - definiše formate poruka za prenos podataka
  2. **SSL protokol dogovaranja parametara sesije** (*SSL handshake protocol*):
     - **za razmenu klijent-server** poruka u prvi put uspostavljenoj SSL vezi
- **SSL protokol podržava više različitih kriptografskih algoritama**

Primer: Autentifikacioni protokoli - SSL

- **Kriptografski algoritmi za komunikaciju SSL protokolom:**

Algoritam	Opis i primena kriptografskog algoritma
DES	*Data Encryption Standard* – standardni algoritam za šifrovanje podataka
DSA	*Digital Signature Algorithm*
KEA	*Key Echange Algorithm* za razmenu simetričnih ključeva
MD5	*Message Digest* v. 5, *hash* funkcija i algoritam za digitalno potpisivanje
RC2 i RC4	*Rivest Ciphers* simetrični kriptografski algoritmi koje je razvio *Ron Riverst*
RSA	Asimetrični algoritam za šifrovanje i autentifikaciju
RSA key exchange	Algoritam za razmenu simetričnih ključeva kod SSL protokola zasnovan na RSA algoritmu
SHA–512	*Secure Hash Algorithm*, *hash* funkcija dužine 512 bita
Triple–DES	*DES* algoritam primenjen tri puta nad istim podacima

Autentifikacioni protokoli – SSL (2)

- **Algoritmi za razmenu ključeva *KEA* i *RSA* *key exchange*** određuju:
  - **klijent- server dogovor simetričnog ključa** za SSL sesiju
  - **najčešće** se koristi ***RSA key exchange*** algoritam
- Tokom uspostavljanja **SSL sesije** (dogovor **Kz** parametara):
  - klijent i server biraju **najjači skup kripto-algoritama**
  - omogućava korisniku da izvrši **autentifikaciju servera**
  - omogućava **klijentu/serveru** da **generišu Pk i Tk sesije**
- Ako **server to zahteva**, SSL protokol dogovara parametre sesije i **omogućava da i server izvrši autentifikaciju klijenta**

Autentifikacioni protokoli – SSL (3)

Ranjivosti:

- **Dolazi u protokolu -TLS** (*Transport Layer Security*)
- Većina SSL implementacija (biblioteka SSL) je **ranjiva na neki način**

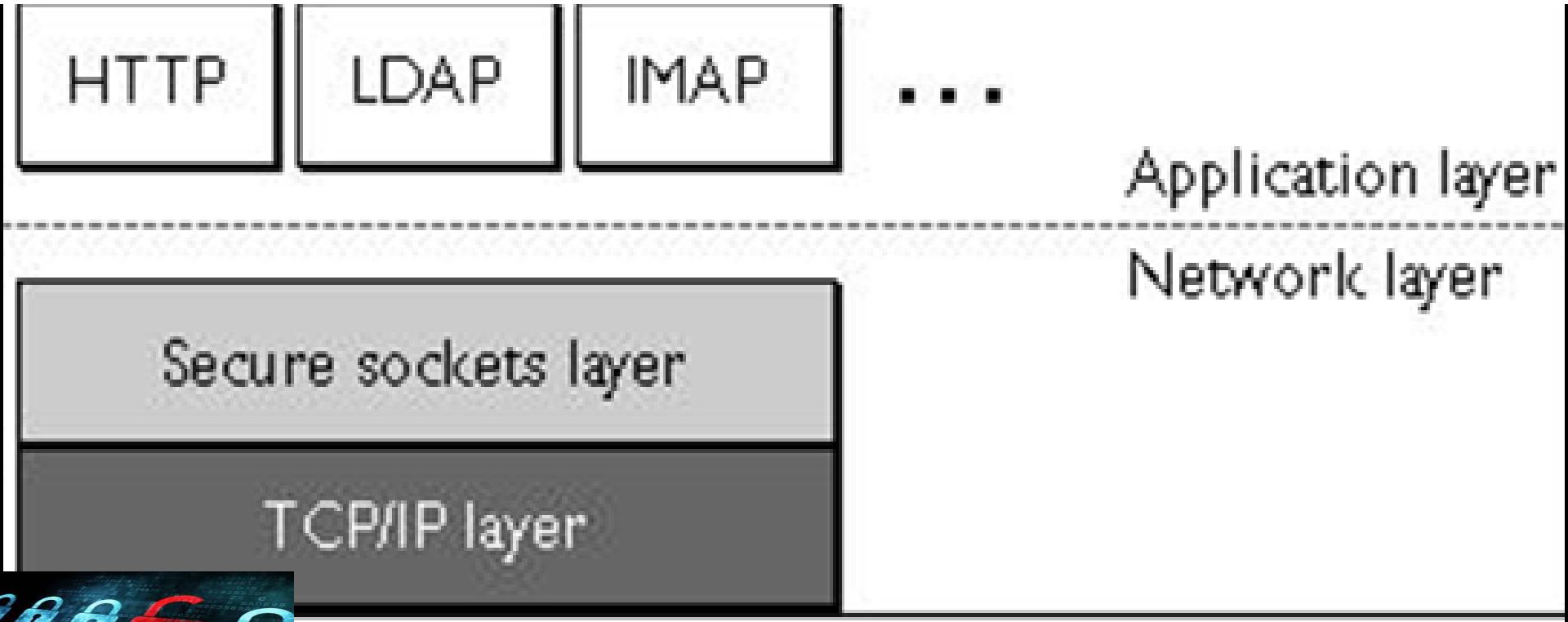
Propust u TLS kodu daje informaciju koja se može koristiti za dešifrovanje korisničkog kukija, ekstrakciju login informacija i krađu sesije, koristeći Java script i prisluškivanje HTTPS (teoretski i statičkog HTTP).

- **Scenario napada** uključuje:
  - **banku** koja koristi protokole zasnovane na veb servisima
  - **korisnika** koji plaća *online* račune
  - **aplikacije** kao što su ***mail* serveri, serveri baza podataka** itd.
  - **napad ubacivanjem čoveka u sredinu** i **otimanjem sesije:**
    - utiče na većinu servera na Internetu
    - **napadač** se **ubaci u SSL protokol** na komunikacionom putu
    - **veb serveri i pretraživači ne mogu otkriti** da je sesija oteta

Primer: Autentifikacioni protokol - **SSL**

1. SSL *(Secure Socket Layer)* protokol obezbeđuje:
- osnovni protokol za **zaštitu pasvorda u prenosu** preko uspostavljene bezbedne sesije (**DES** alg.)
- često se koristi **za pristup *web* aplikacijama** na Internetu
- nije stvarni primer *autentifikacionog protokola*

- **Položaj SSL protokola u OSI** arhitekturi RM:



Autentifikacioni protokoli tipa *upit-odgovor*

- Većina autentifikacionih protokola su tipa *upit-odgovor*
- Zahtevaju uspostavljanje PKI ili TTP servisa:
  - korisnik (klijent) se loguje na sistem (server)
  - sistem (server) zahteva dokaz o identitetu korisnika
  - korisnik (klijent) se za pristup **identifikuje sistemu**
  - sistem odgovara sa **slučajnim upitom** (*chalange*)
  - **korisnik šifruje upit** svojim **Tk** i **šalje ga nazad** sistemu
  - sistem koristi **Pk** korisnika za dešifrovanje
- **Protokol *Kerberos*** je:
  - tipa upit odgovor
  - **koristi TTP servis** umesto **PKI** sistema

Autentifikacioni protokol - Kerberos

- **Kerberos** se zasniva na upotrebi **N simetričnih ključeva** za **N** korisnika
- Ne mora da postoji PKI sistem, ali **zahteva TTP servis**
- **TTP** je **Centar za distribuciju ključeva - KDC** (*Key Distribution Center*)
- **Master ključ –K_{KDC}** je tajna koju zna samo **KDC**
- **KDC** vrši autentifikaciju, generiše i deli **simetrične sesijske ključeve -Ki** za zaštitu **poverljivosti i integriteta**
- Mogu se koristiti **različiti simetrični** algoritmi

Autentifikacioni protokoli – Kerberos (1)

- **KDC** izdaje:
  – **Tiket -** informacije potrebne za pristup servisu RM
- Klijent koristi **TGTs** (***Ticket-granting tickets)*** da dobije **tiket**
- **Svaki TGT sadrži**:
  - *sesijski ključ* **K**
  - *korisnički* **ID**
  - *vreme validnosti*
- **Svaki TGT je šifrovan sa K_{KDC}**
  - jedino **KDC** može da pročita **TGT**

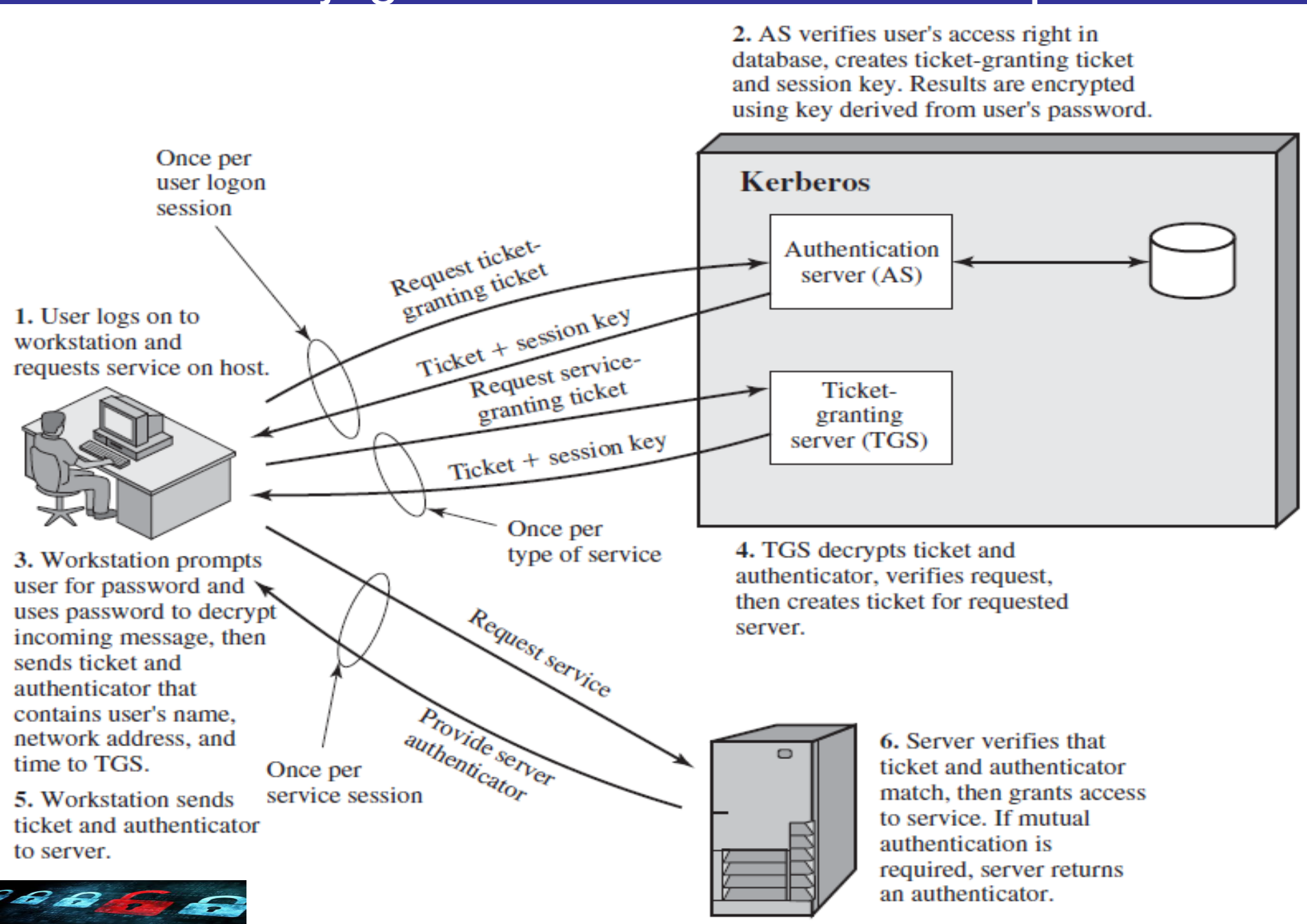
Autentifikacioni protokoli – Kerberos (2)

- Da bi se **ulogovao korisnik A** unosi lozinku **“A”**
- **Lozinka korisnika “A”** traži **TGT**
- **Računar korisnika A (KDC)**:
  - izdvaja ključ $\mathbf{K_A}$ iz lozinke korisnika A **(“A”)**
  - **KDC** koristi ključ $\mathbf{K_A}$ da bi korisniku **A** poslao **TGT:**
    - **KDC** kreira sesijski ključ $\mathbf{S_A}$
    - **KDC** šifruje: $\mathbf{E(S_A, TGT, K_A)}$
    - Računar **A** dešifruje poruku **KDC** i briše $\mathbf{K_A}$:

$$\mathbf{TGT = E(“A”, S_A, K_{KDC})}$$

- Korisnik **A**, koristi svoj **TGT** (potvrdu) za bezbedan pristup sistemu
- **Pozitivno**: *Korisnik A nema mnogo posla oko procedure pristupa*
- **Negativno**: **KDC mora biti od apsolutnog poverenja**!

Primer: Dijagram aktivnosti Kerberos protokola



Autentifikacioni protokoli - *Ranjivosti*

- Ako **upit nije slučajna vrednost**:
  - napadač ga **može presresti (“***čovek u sredini***”)**
  - **lažno se predstaviti** i izdati novu vrednost upita
  - **primiti transformisani odgovor** i
  - **obezbediti neovlašćen pristup** sistemu

Primer:

Kerberos (*Windows NT 4.0 OS*) *Needham – Schroeder* ima ranjivost-pristup RS **korišćenjem starog ključa K_A**

Autentifikacioni uređaji

- **Fizički identifikator:**
  - za prenos/skladištenje **autentifikacionih podataka**
- **Kriterijumi za izbor**:
  - *performanse i pouzdanost, pogodnost za primenu*, *korisnička sposobnost i prihvatljivost i cena nabavke*
- **Većina spada u kategorije**:
  - *smart kartica*
  - HSM (hardversko softverskih modula)
  - *biometričkih uređaja i tokena i*
  - *drugih autentifikacionih uređaja*

1. Smart kartice

- **Koriste se za:**
  - **visoku bezbednost IS sa HSM**
  - zaštitu **kriptografskih tajni**
  - **bezbedno skladište kripto-ključeve** korisnika
- **Sa aspekta fizičkih karakteristika postoje**:
  - ***kontaktne smart kartica***
    - zahtevaju fizički kontakt sa čitačem kartica
  - ***beskontaktne smart kartica***
    - Kapacitivno/induktivno spregnute sa čitačem
  - ***kombinovane smart kartica***
    - obezbeđuju oba načina rada

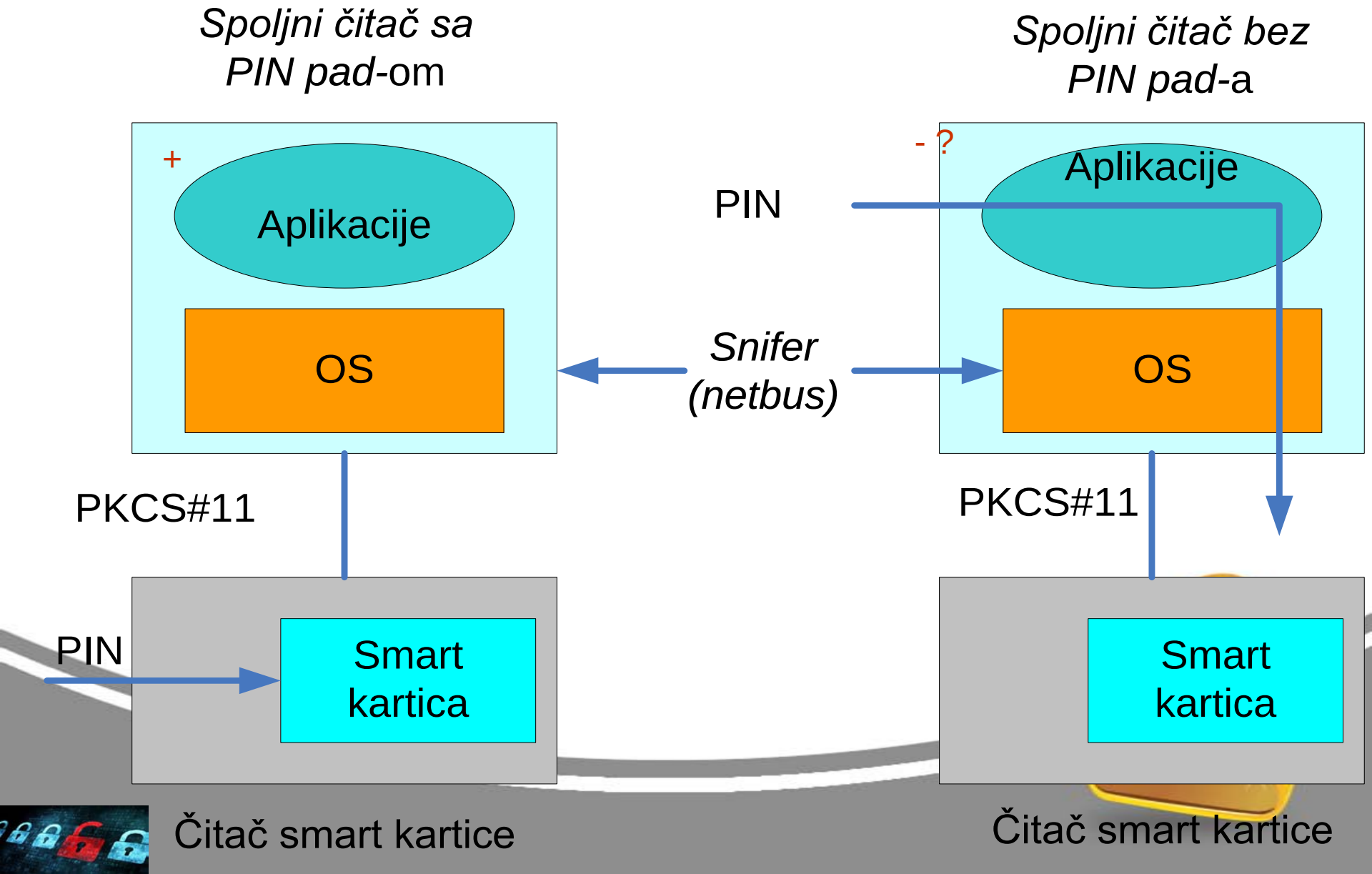
1. Smart kartice (2)

- **Sa aspekta funkcionalnosti postoje:**

1. **Memorijske *smart* kartice:**
   - skladište ključ za kriptografske operacije u RS
   - *kriptografske operacije se izvršavaju izvan kartice*
2. **Mikroprocesorske (kriptokartice) *smart* kartice** :
   - **skladište ključeve** na kartici (trajno)
   - *kriptografske operacije se vrše na kartici* preko API interfejsa npr. ***PKCS#11, PC/SC, OCF i CDSA***
   - problem kod implementacije rešenja (**primer**):
     - *PIN ne sme prolaziti kroz OS*
     - *zahteva se eksterni čitač PIN-a*

Primer: Kriptokartica sa eksternim čitačem kartica

PIN ne sme prolaziti kroz OS!



1. Smart kartice (3)

- **Generalno se smatraju bezbednim za skladištenje**:
  - *kriptografskih ključeva i*
  - *drugih poverljivih informacija korisnika*
- U velikoj meri su **doprinele razvoju koncepta e-plaćanja**
- **Bezbednosne ranjivosti** *smart* kartice - napadi :
  - *diferencijalnom analizom snage napajanja* i
  - *optičkom indukcijom greške*
- **Kriptografske aplikacije** koriste *smart kartice*

2. Kriptografski moduli HSM
(*Hardware Security/Storage Module)*

- **HSM na serverskoj strani** su bolja opcija
- **Važan standard za HSM** - **NIST FIPS 140-1** i **2**:
  - pokriva ukupno **11** oblasti dizajna i implementacije
  - rangira nivoe bezbednosti na **4 nivoa**:
    - **1. nivo -** *najmanje zaštite*
    - **4. nivo –** *najveći nivo zaštite*
- **Kriptografski akceleratori** – specijalizovani ***HSM*** :
  - za e-biznis, **opslužuje neograničen broj klijenata**
  - ima **veću skalabilnost aplikacija** i Kz rešenja

3. Biometrijski uređaji

- **Mehanizmi AC RM/RS uvek su kompromis između**:
  - **potrebe za zaštitom** i
  - **potrebe za komfornim pristupom** regularnih korisnika
- **Biometrijski uređaji verifikuju identitet korisnika** na bazi:
  - jednog ili više fizičkih atributa biometričkih parametara
- ***Biometrika* obuhvata tehnike provere**:
  - *otiska prsta,*
  - *geometrije ruke,*
  - *mrežnjače oka, DNK,*
  - *prepoznavanja govora, lica, facijalne termografije*...

3. Biometrijski uređaji -1

- **Kriterijumi za izbor biometrijskih tehnika**:
  - *performanse i pouzdanost, pogodnost za primenu*
  - *kompleksnost korisničke upotrebe*
  - *sposobnosti korisnika i korisnička prihvatljivost*
  - *troškovi nabavke i dr.*
- **Problemi biometrijske autentifikacije**:
  - *visoka cena, korisnička neprihvatljivost,*
  - *visok stepen grešaka, teška autentifikacija uređaja*
  - *neotpornost na napade* (npr. otisak prsta) i dr.

3. Tokeni

1. **Uređaje za bezbedno skladištenje kripto- informacija**
   - alternativa *smart* karticama
2. **Priručni uređaj za autentifikaciju**
   - sa malim **displejom i tastaturom**
   - **ne moraju** se **povezivati na radnu stanicu**
   - konfiguriše se sa **A** serverom pre izdavanja prava pristupa
   - **A** server i token razmenjuju kriptografske tajne
   - korisnik unosi **lozinku** ili **PIN** za **pristup tokenu**
   - **token na displeju prikaže A podatke** za pristup
   - korisnik **ove podatke unosi u svoj RS** i kompletira proces **A**

Primer: Ostali autentifikacioni uređaji i protokoli

- **MEDIA protokol** (*patent US Br. 7.577.987*, **2009**)
- **Metod generisanja ključeva za komunikacionu sesiju šifrovanja i sistem autentifikacije***:*
- Koristi mehanizam za **dvoslojnu uzajamnu autentifikaciju i bezbednu sesiju za distribuciju slučajnog simetričnog ključa**
- **Podržava B2B i B2C mreže e–trgovine** i upotrebu uređaja:
  - mobilnih, laptop/desktop računara, ATM, POS terminala, VOIP, GPS i dr.

Primer: Ostali autentifikacioni uređaji i protokoli

- **MEDIA** koristi algoritme zasnovane na **3 tehnologije**:
  - **TILSA** (*Time Interplay Limited Session Random Key*): **algoritam za generisanje ključa**
  - **KEDIA** (*Key Encryption/Decryption Iterative Algorithm*): **protokol za razmenu ključa koristi TILSA algoritam** i autentifikacione parametre strana u komunikaciji sa iterativnim algoritmom za ključ za šifrovanje/ dešifrovanje
  - **KCA** (*Key Conversion Array*) za **konverziju ključa** i **visok nivo zaštite** poruka preko nepoverljivih linija (**Kz algoritmi**: *Bit–Veil–Unveil* (**BitVU**), *Byte–Veil–Unveil* (**ByteVU**) i *Bit–Byte–Veil–Unveil* (**BBVU**)

Serveri za autentifikaciju i autorizaciju (*SA&A)*

1. **Autentifikacioni serveri** centralizuju upravljanje identiteta u RM

   PRIMER: Primarni kontroler domena (*PDC*) *u Windows* OS za *Win* klijente u LANu

2. **Autorizacioni serveri** pridružuju skup privilegija autentifikovanim entitetima
3. **SA&A-za kontrolu udaljenih pristupa** obezbeđuju:
   - **servise za više klijenata** u klijent-server arhitekturi
   - **pristupe svim apstraktnim slojevima programa**
   - mogu **dodeljivati uloge** korisnicima **(Npr., *CISCO A&A*)**

Tipičan primer *SA&A*

1. **NAS** (*Network Access Server*) – **server za mrežni pristup**:
   - **primenjuje restrikcije** i dopušta udaljenu konekciju
   - udaljeni korisnik preko **PSTN** šalje identifikaciju serveru
   - može koristiti lokalnu b/p ili, **servise namenjene** za **SA&A**
- **Serverska konfiguracija:**
   - **posrednik između korisnika i servera** (p/i, servisa)
   - **prenosi svaki zahtev** od klijenta prema serveru i odgovara
   - **server** sa dovoljno podataka **prihvata/odbija zahtev** klijenta
   - **server šalje odgovor NAS**-u
   - **NAS** izvršava odluku prema skupu predefinisanih pravila

Autentifikacioni i autorizacioni protokoli

- **Fleksibilnost metoda A&A** postiže se implementacijom:
  - **standardnog protokola** na nivou aplikacija **između NAS i bezbednosnog servera**
- **Protokoli podržavaju generičku razmenu između NAS i servera koji ne zavisi od procesa A&A**
- **Postoje dva glavna protokola koji se danas koriste:**
  - **RADIUS** (*Remote Authentication Dial In User Service*)
  - **TACACS +** (*Terminal Access Controller Access Control Service*) protokol

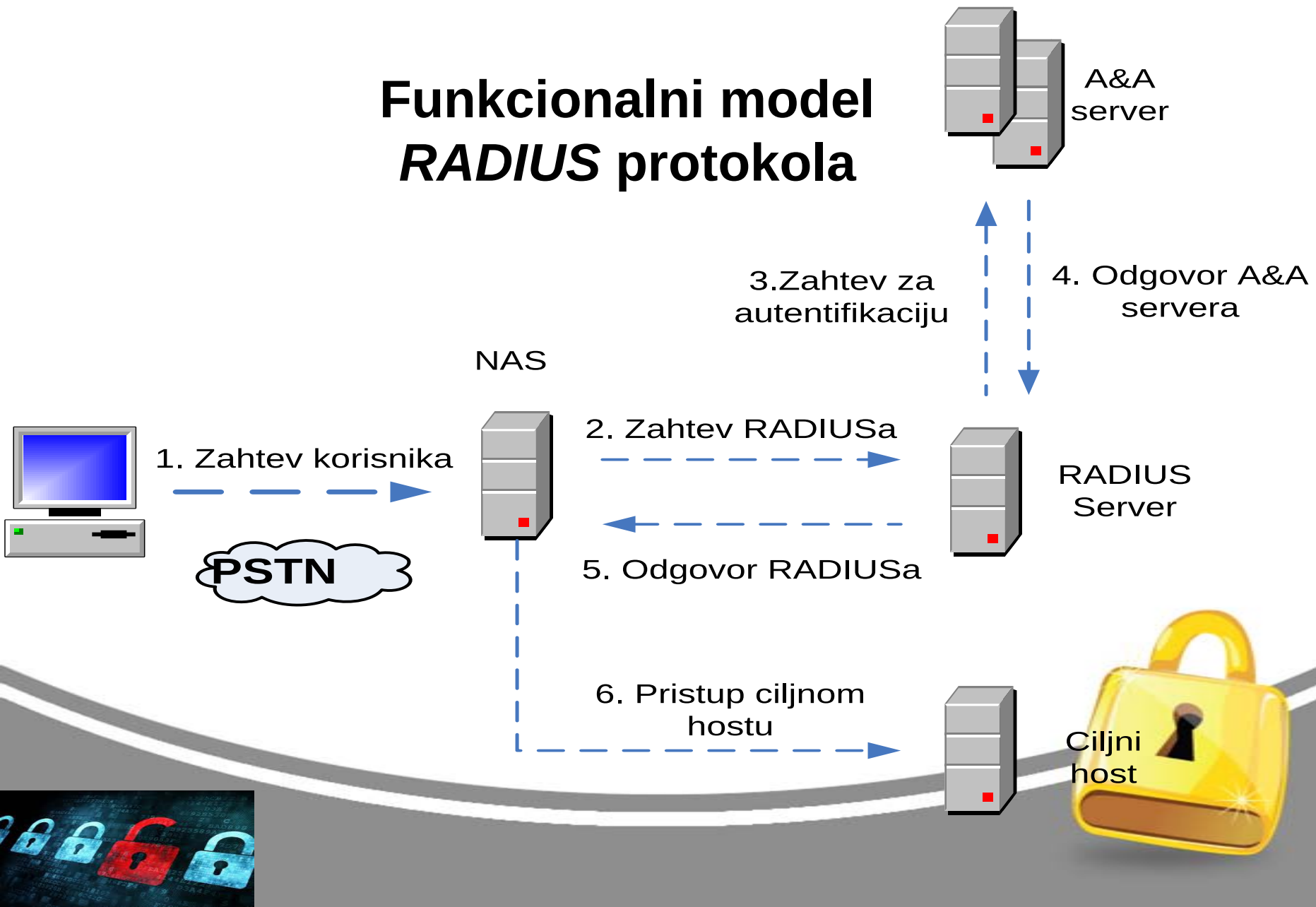
Autentifikacioni i autorizacioni protokoli

- **Vrlo su sličnih funkcionalnosti, a osnovne razlike su:**

RADUUS	***TACACS+***
izvršava se preko **UDP**	izvršava se preko **TCP** protokola
sadrži korisnički profil za autentifikaciju sa svim parametrima korisnika	razdvaja autentifikaciju i autorizaciju
koriste ga **računari i mrežni uređaji**	koriste ga mrežni uređaji (**ruteri, svičeri**)

Primer: Protokoli za razmenu između NAS i servera

Funkcionalni model *RADIUS* protokola



Funkcionalni model RADIUS protokola

- Korisnik **inicira *dial-up* vezu sa NAS** serverom
- **NAS traži korisničko ime i lozinku**
- **NAS** je **RADIUS *klijent* i** šalje zahtev za pristup **RADIUS serveru**
- **RADIUS server prenosi autentifikacione podatke na A&A server** (može i autorskim protokolom)
- **Server za A&A dopušta/odbija zahtev** korisnika
- **RADIUS server odgovara NAS–u** sa porukom da prihvata/odbija pristup
- **Ako je autentifikacija uspešna, NAS server dopušta pristup** ciljnom hostu

Bezbednost SA&A

- Značajno povećava bezbednost pristupa udaljenih korisnika
- **Stvarni nivo bezbednosti RM zavisi od metoda A&A**:
  - *pasvord* – nizak nivo zaštite
  - *Kz mehanizam upit-odgovor tipa* – **viši nivo zaštite**
  - *jednokratni pasvord* (kriptokartica) - **najviši nivo zaštite**
- **Tehnika A&A ne štite podatke između korisnika i hosta:**
  - *zaštitni protokol između korisnika i terminala iza NAS*
  - *štiti poverljivost podataka i integritet same sesije*
- **Za *web* aplikacije**:
  - **EAM** (*Extranet Access Management*) protokol
  - **obezbeđuje servise A&A** u Internet okruženju (suprotno udaljenom pristupu)

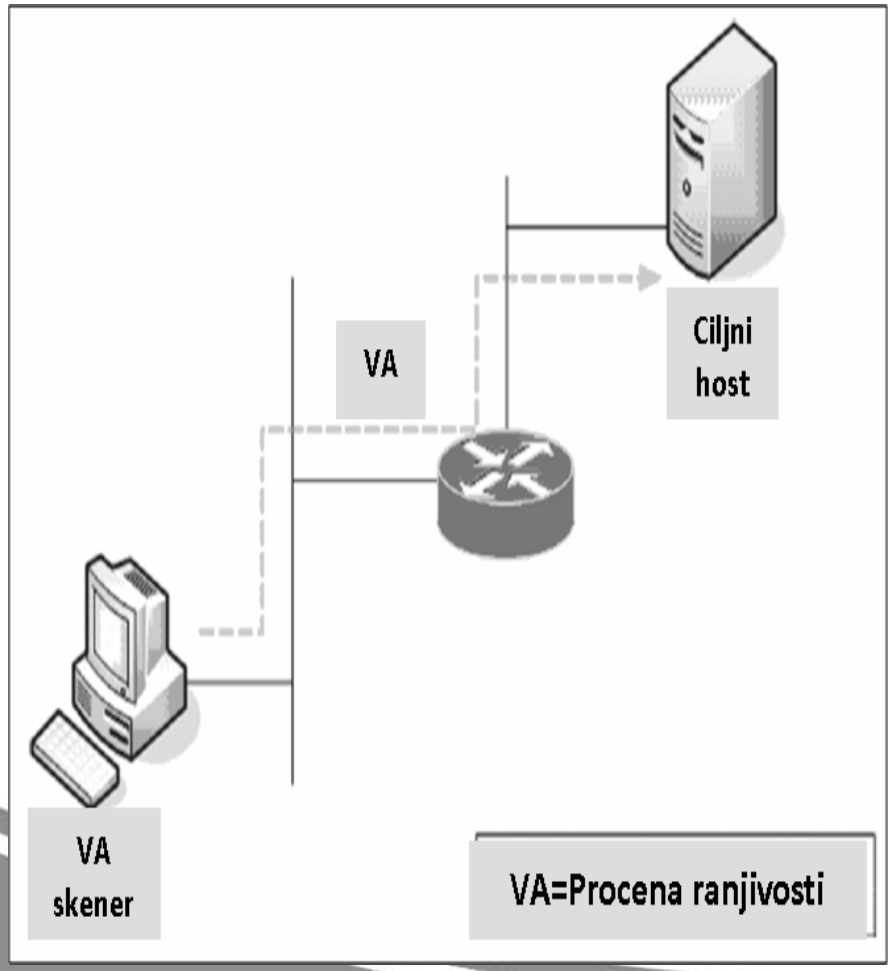
Integritet RM
-Skeneri zaštite RM-

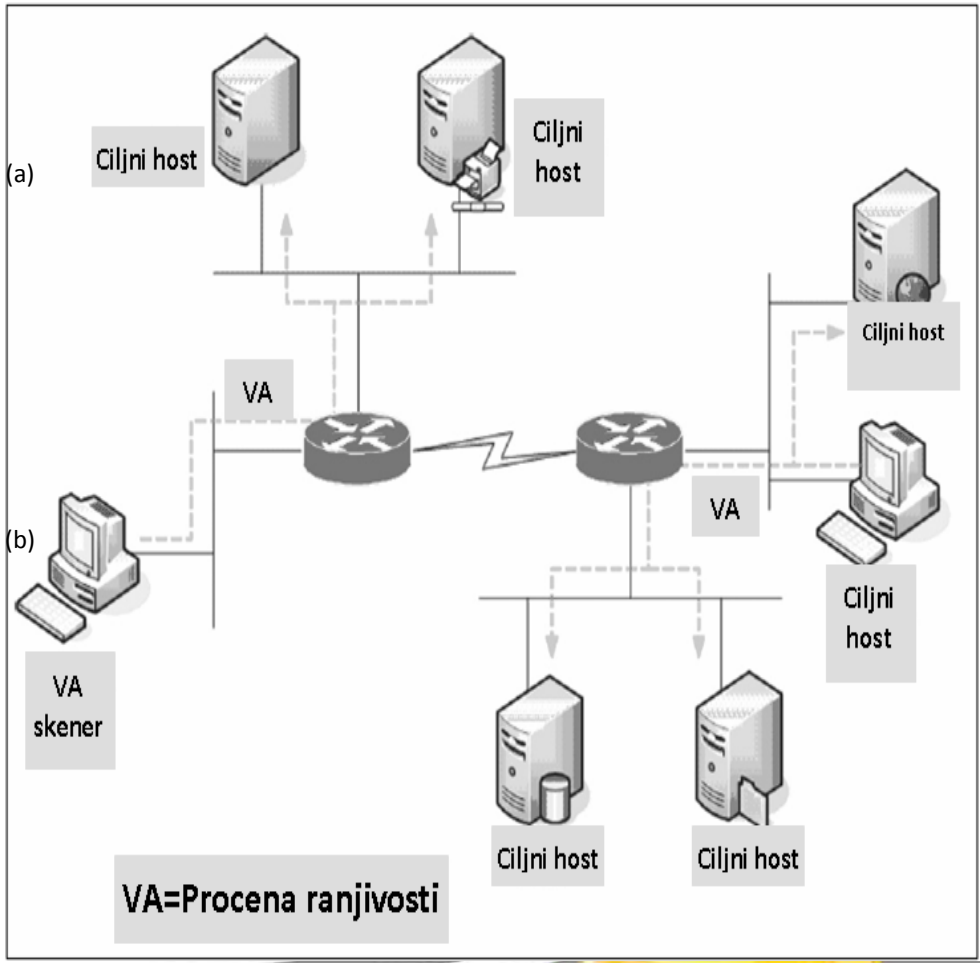
- **Kao *skeneri zaštite RS,* otkrivaju ranjivosti RM**:

1. **Najjednostavniji skener RM mapira uređaje u RM sa*:***
   - **ICMP** (*Internet Control Message Protocol*) ***pinguje***
   - **ICMP** koristi **OS RM** za slanje grešaka u **IP** datagramu
2. **Na višem nivou - mapiraju portove, pinguju** TCP/UDP
3. **Mapiraju RM i identifikuju servise** (*vulnarability scaners*)
4. **Komercijalni alati** sadrže b/p sa **poznatim ranjivostima**:
   - upoređuju aktuelnu konfiguraciju sa predefinisanom
   - izveštavaju više vrsta informacija sa manje detalja

Primer: Arhitektura skenera za procenu ranjivosti

(a) RS u mrežnom okruženju (b) RM



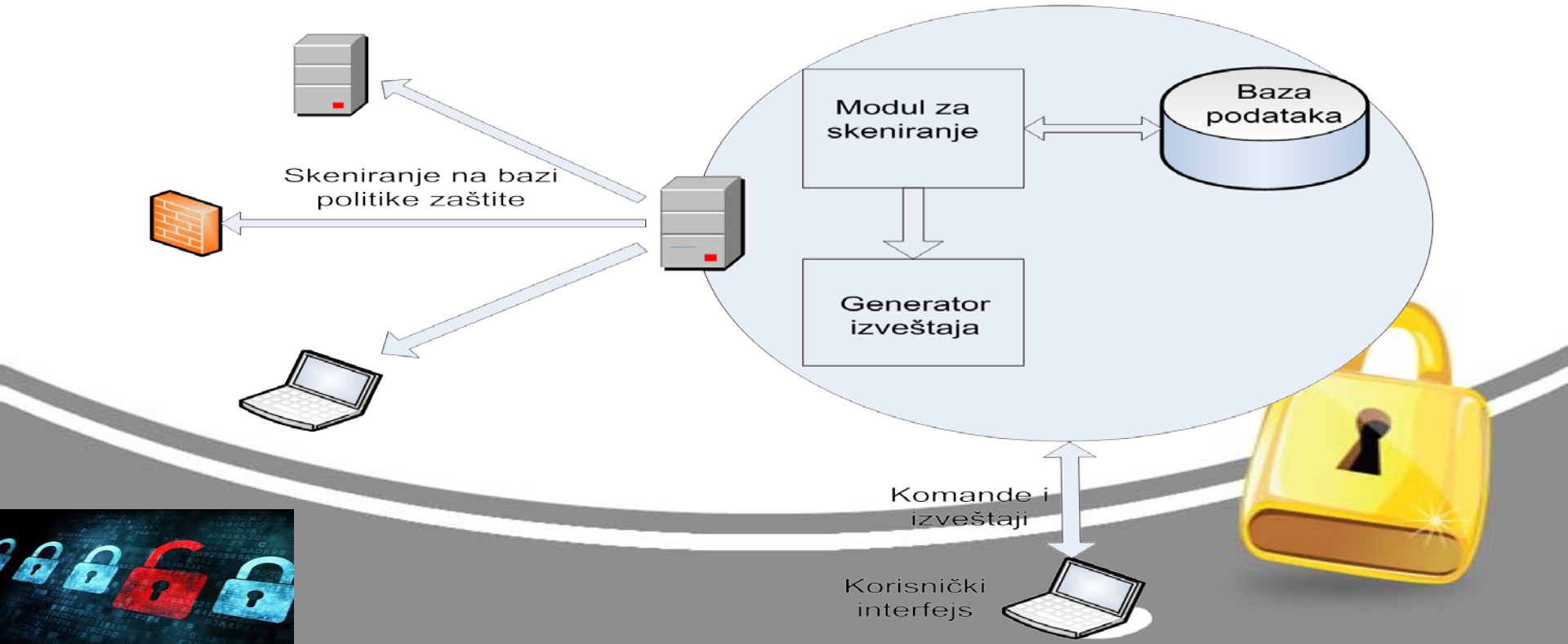


(a)

(b)

Primer: Arhitektura skenera ranjivosti RM

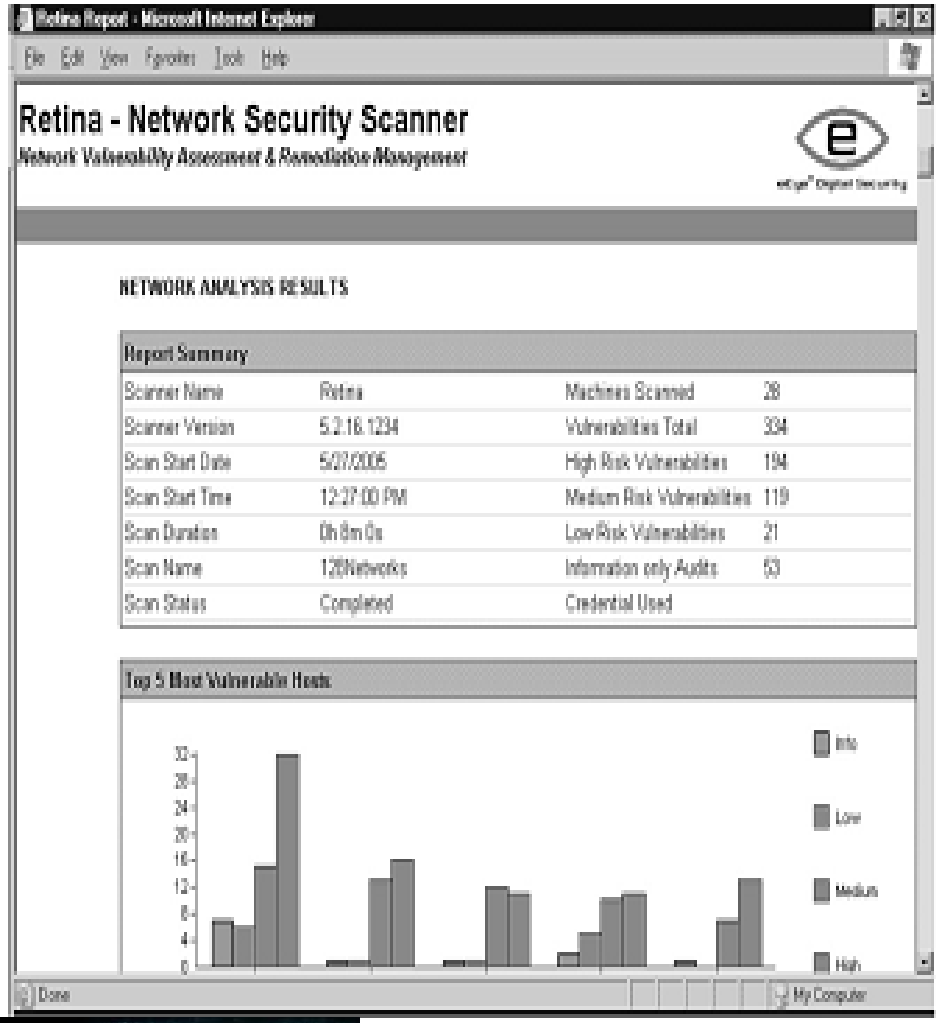
- **Arhitektura skenera ranjivosti RM uk**ljučuje:
  - *modul za skeniranje,*
  - *bazu podataka sa definicijama poznatih ranjivosti,*
  - *modul za generisanje i prezentaciju izveštaja i*
  - *korisnički interfejs*



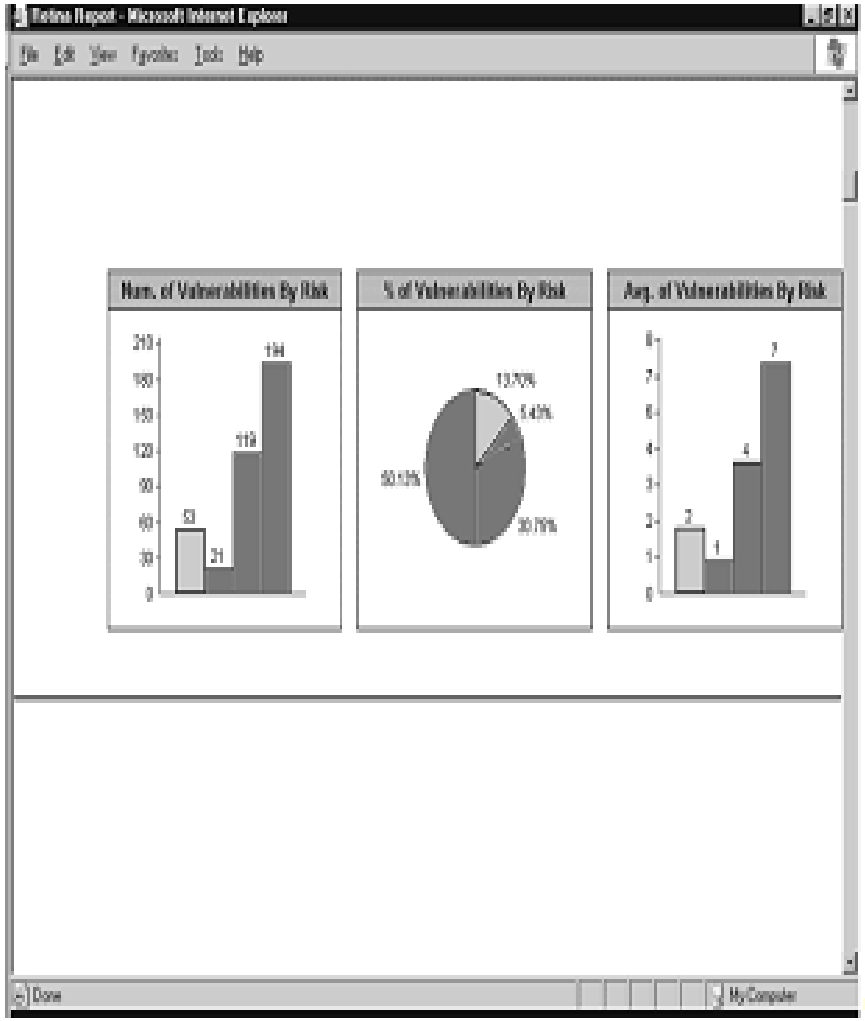
Primer: *Retina–Network Security Scanner*

Rezultati analize ranjivosti – (a)

Tipovi izveštaja – (b)

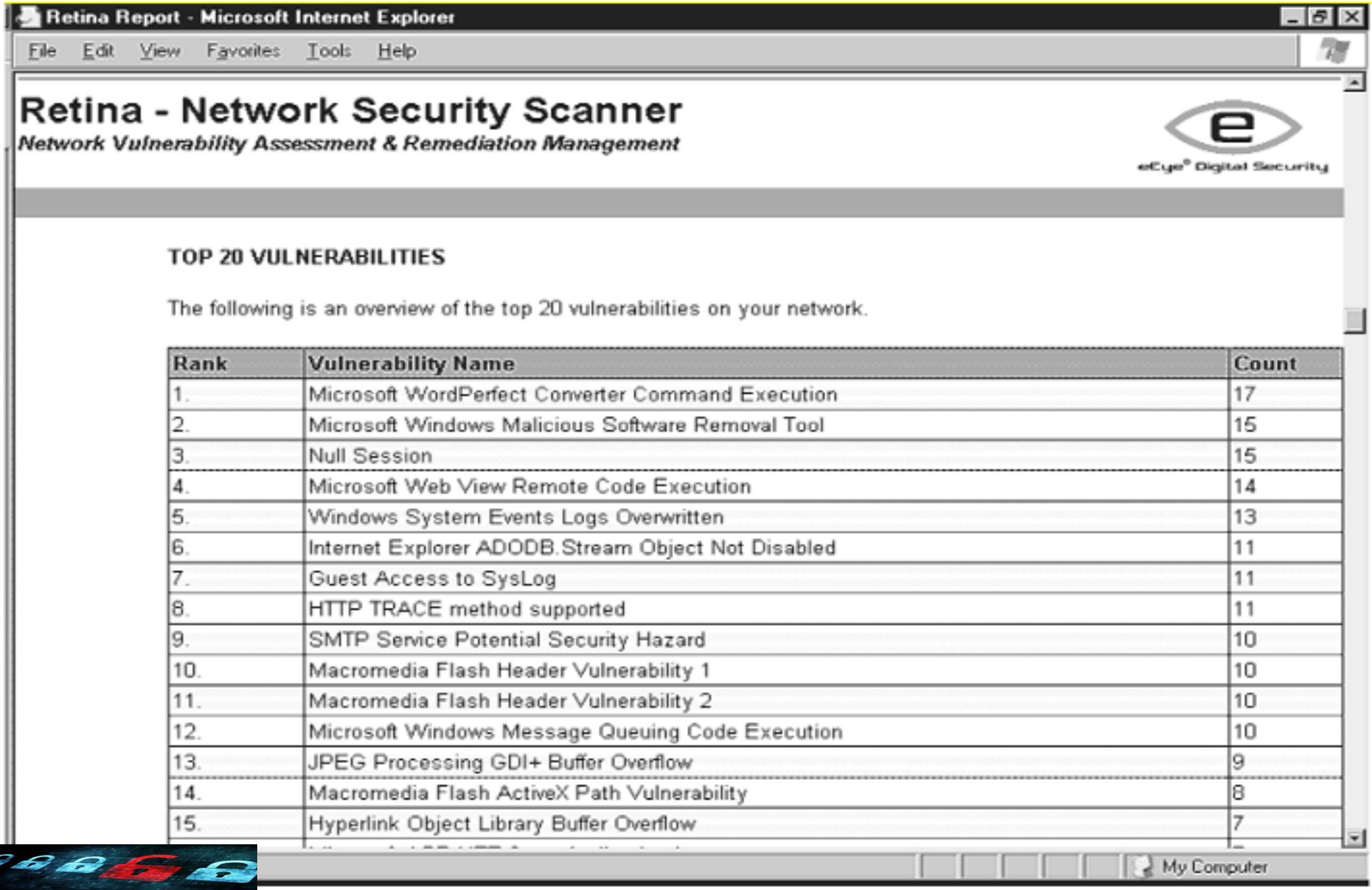


(a)



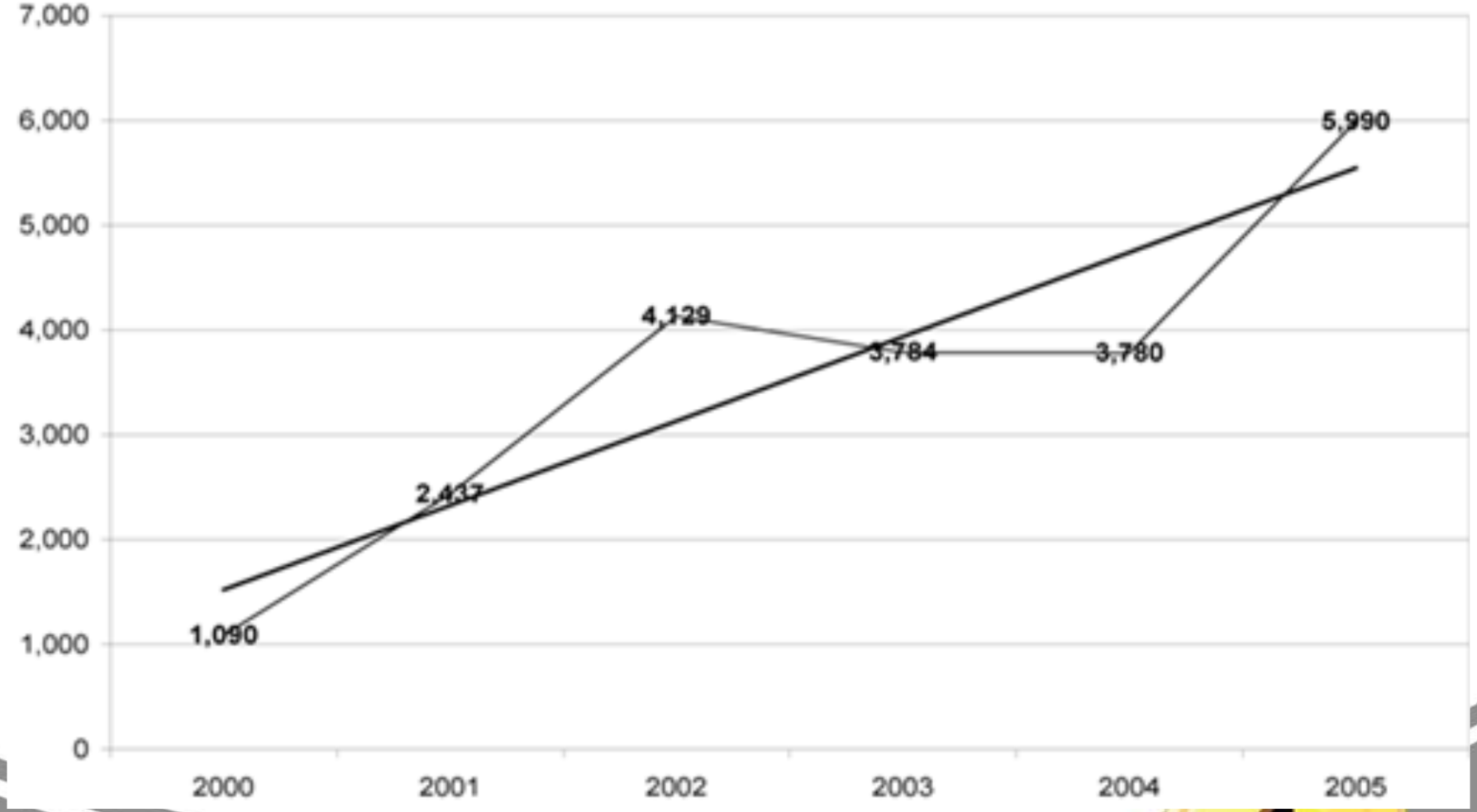
(b)

Primer: *Retina–Network Security Scanner*
- Glavne ranjivosti RM (2006) -



Rank	Vulnerability Name	Count
1.	Microsoft WordPerfect Converter Command Execution	17
2.	Microsoft Windows Malicious Software Removal Tool	15
3.	Null Session	15
4.	Microsoft Web View Remote Code Execution	14
5.	Windows System Events Logs Overwritten	13
6.	Internet Explorer ADODB.Stream Object Not Disabled	11
7.	Guest Access to SysLog	11
8.	HTTP TRACE method supported	11
9.	SMTP Service Potential Security Hazard	10
10.	Macromedia Flash Header Vulnerability 1	10
11.	Macromedia Flash Header Vulnerability 2	10
12.	Microsoft Windows Message Queuing Code Execution	10
13.	JPEG Processing GDI+ Buffer Overflow	9
14.	Macromedia Flash ActiveX Path Vulnerability	8
15.	Hyperlink Object Library Buffer Overflow	7

Primer: *Linearna aproksimacija rasta ranjivosti*



Skeneri telefonskih veza

- **Razvijeni iz hakerskih sw alata tzv**. ***war dialing*** za identifikovanje ranjivosti IS preko telefonske linije
- **Konstruišu bezbednosnu mapu tel. sistema** org.
- **Detektuju neovlašćene i nepoznate modeme u LAN**
- **Kombinuju *pingovanja* i *prompts*** o ranjivostima OS
- Automatizacija povećavaa detekciju neovlašćenih modema
- **Sofisticirani, jednostavan GUI, različite izveštaje i** daju:
  - **specifikaciju brojeva** za skeniranje
  - **programiranje rada**

Pitanja