V – Sigurnosne arhitekture i protokoli

S A D R Ž A J

1. Sigurnosne arhitekture
2. Implementacija zaštite u TCP/IP steku
3. IPSEC protokol
4. Protokol Secure Sockets Layer(SSL)

5.1 - Sigurnosne arhitekture

- Sigurnosna arhitektura informacionog sistema predstavlja osnovu za sprovođenje sigurnosne politike svake organizacije.
- Zavisi od stepena sigurnosti koji želi da se postigne kao i o tipu sistema: zatvorenom, otvorenom, centralizovanom ili distribuiranom
- Na osnovu toga gradi se odgovarajuća sigurnosna arhitektura i primenjuju se odgovarajuće metode zaštite.
- Kombinacija zatvorenog–centralizovanog sistema je najjednostavnija i najpouzdanija za realizaciju sa stanovišta bezbedonosti, dok otvoreni-distribuirani sistem zahteva mnogo više napora i podložan je sigurnosnim propustima koje je potrebno permanentno tražiti i krpiti.
- **Otvoreni sistemi** kao svoju prednost imaju nezavisnost od proizvođača, kompatibilnost sa svima koji su prihvatili određene specifikacije i interfejse i dostupni su svim zainteresovanima
- **Zatvoreni sistemi** su u vlasništvu proizvođača koji je u obavezi da obezbedi softversku i hardversku podršku koja je najčešće nekompatibilna sa svim ostalim tako da je praktično nemoguće da se koriste proizvodi drugih

5.1 – Sigurnosne arhitekture

- Bez obzira kojem tipu pripadao, jedan sistem bi trebalo da poseduje tri zaštitna mehanizma:

  -računarska baza od poverenja (*Trusted Computing Base*), koja obuhvata zaštitne mehanizme unutar računarskog sistema i uključuje hardver, softver i firmver a ima ulogu primene sigurnosnih pravila

  -sigurnosni perimetar (*Security Perimeter*), predstavlja granicu između baze od poverenja i ostatka sistema

  -nerizičan put (*trusted path*), koji obezbeđuje korisniku da pristupi bazi od poverenja tako da ga pri tome ne mogu kompromitovati drugi procesi ili korisnici.
- Računarski sistem od poverenja jeste onaj koji koristi nužne mere obezbeđenja hardvera i softvera kako bi omogućio obradu informacija
- U njemu može biti aktivno više procesa, a svaki od procesa ima pristup određenim memor. lokacijama i mogućnost da izvršava CPU naredbe
- Izvršavanje procesa i memorijsko područje koje je dodeljeno svakom procesu zove se ***zaštitni domen*** (*protection domain*).

5.1 – Sigurnosne arhitekture

- Informacioni sistemi rade u različitim sigurnosnim režimima koji su određeni nivoima klasifikacije informacija, profilima korisnika i njihovim ovlašćenjima:
- ***Visoki sistemski režim*** -imaju ovlašćenja ali ne znaju/vide sve podatke.
- ***Multi level režim rada*** - podržava korisnike na različitim nivoima i podatke različitih nivoa klasifikacije.
- ***Namenski*** - korisnici znaju sve informacije u sistemu, sistem može da radi sa više klasifikacionih nivoa.
- ***Odeljeni*** - korisnici imaju najviša ovlašćenja ali nemaju sva prava
- ***Kontrlisani*** - postiže se ograničeni nivo poverenja u kombinaciji sa različitim nivoima klasifikovanosti.
- ***Ograničeni pristup*** - za rad sa korisnicima koji nisu sigurnosno provereni.

5.1 - Sigurnosne arhitekture

- Ranjivost u sistemskoj sigurnosnoj arhitekruri mogu voditi ka narušavanju sistemske sigurnosne politike.
- U običajene ranjivosti sigurnosne arhitekture spada:

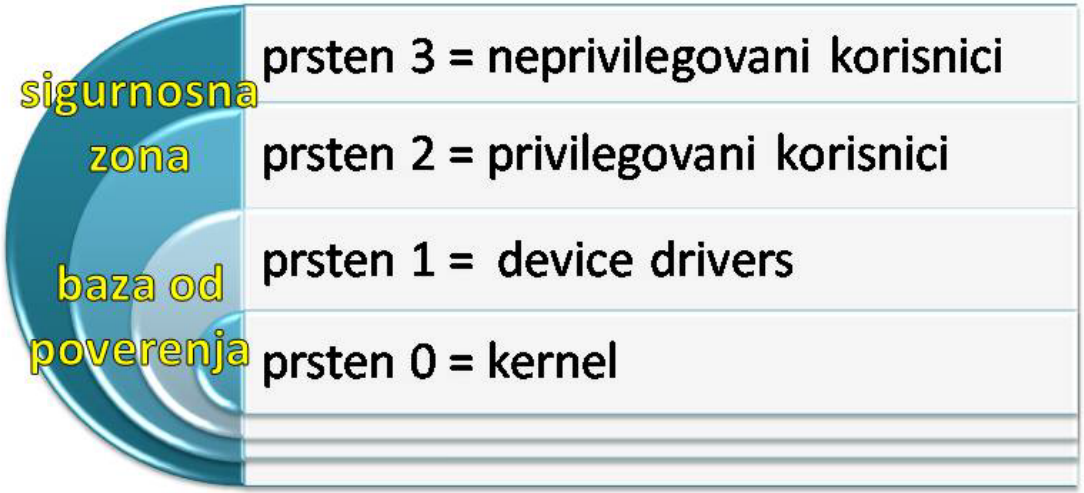
1. ***Skriveni kanal*** - Nenamerni komunikacioni kanal između dva ili više subjekata koji dele zajednički kanal.
2. ***Nepostojanje provere perimetara*** - Greška ili nepostojanje provere ulaznih tokova koji su određeni parametrima.
3. ***Maintenance hook ranjivost*** - Sistem za održavanje koji preskače sisteme zaštite.
4. ***Time of Check to Time of Use(TOC/TOU) napad*** - Napad koji isorišćava razliku između vremena kada su sigurnosne kontrole primenjene i vremena kada je korišćena usluga provere identiteta i iskorišćeno neko pravo.

5.1 – Sigurnosne arhitekture

- Jedna od šema koja podržava višestruke domene zaštite jeste korišćenje ***zaštitnih prstenova***.
- Prstenovi su realizovani tako da domen s najvećim pravima u centru prstena, a domen s najmanjim pravima spoljašni.
- Jezgro operativnog sistema obično se nalazi u prstenu 0 i ima pravo da pristupi svim domenima u sistemu.
- ***Sigurno jezgro*** (*security kernel*) čine hardverski, firmverski i softverski elementi računarske baze od poverenja, koji implementiraju koncept monitora referenci (*reference monitor*).
- ***Monitor referenci*** je sistemska komponenta koja forsira kontrolu pristupa objektima.
- Sigurno jezgro mora da: posreduje u svim pristupima, bude zaštićeno od izmena i bude verifikovano kao ispravno.
- ***Sigurnosna oznaka*** ukazuje na potrebu za posebnim načinom (režimom) rukovanja ili se može koristiti za kontrolu pristupa.

5.1 - Sigurnosne arhitekture

- Ovi apstraktni tipovi su našli svoju implementaciju u mehanizmu zaštitnih prstenova koji je prvi put primenjen u MIT-ovom operativnom sistemu **MULTICS** (projektovan 1964. godine).
- On je bio projektovan da sadrži 64 prstena od kojih je realizovano 8.
- U ovakvoj hijararhiji baza od poverenja se nalazi na nultom prstenu i u njemu se nalazi jezgro operativnog sistema (*kernel*).
- U njemu se formira monitor referenci (*reference monitor*) koji posreduje prilikom interakcije sa objektima i koji se nalazi na prelazu nultog ka prvom prstenu.
- Sigurnosna zona bi trebalo da obuhvati bar dva prstena od kojih se jedan odnosi na pristup niskom nivou od strane ovlašćenih korisnika odnosno u drugom su neprivilegovani korisnici.



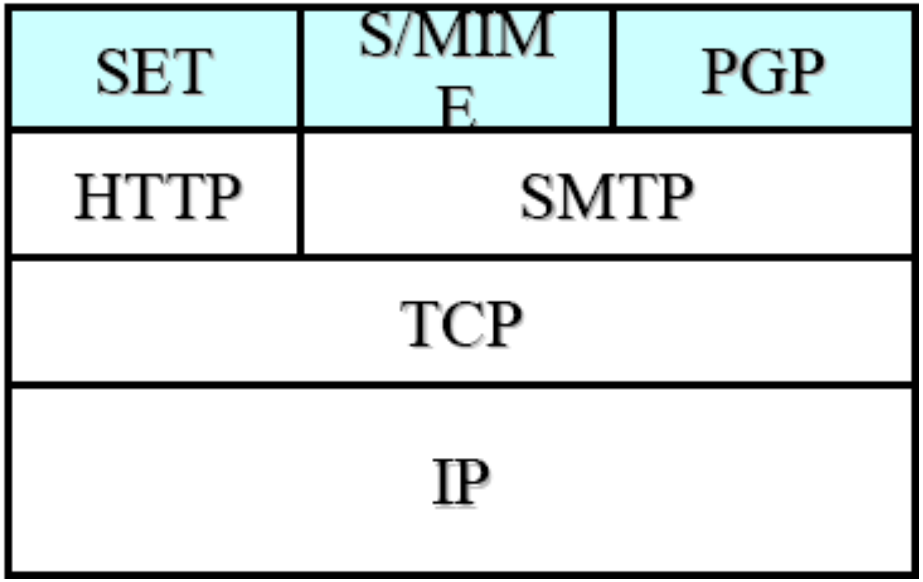
5.1 - Sigurnosne arhitekture

- Sve ovo je primenljivo kod računara koji su deo centralizovanog modela organizovanja ali ne važi za distribuirani model
- Tu su korisnici najčešće mobilni, sa različitim OS i stepenima zaštite koji pored obavljanja posl.zadataka koriste računare i za druge aktivnosti
- Ovde se ne mogu potpuno zaštititi sistemi i zato se koriste određene norme i pravila kako bi se napadačima otežao posao.
- Ta pravila se najčešće odnose na:
  - pravila o elektronskoj pošti i razmeni datoteka
  - prijavljivanje korisnika koje se vrši preko biometrijskih podataka
  - GUI (*Graphical User Interface*) se projektuje tako da ograničava pristup određenim podacima
  - vrši se šifrovanje sadržaja i prenosa
  - vrši se centralizovana izrada rezervnih kopija
  - vrši se kontrola instaliranog softvera
  - vrši se kontinuirana edukacija korisnika o mogućim sigurnosnim propustima, itd.

5.2 - Sigurnosne arhitekture

Sloj aplikacije.

- Na ovom nivou zaštita se vrši u samoj aplikaciji tako da svi slojevi ispod prenose već zaštićenu poruku koja kao takva ide krajnjem korisniku koji na inverzan način dobija original.
- Prednost ovakve zaštite je nezavisnost od sigurnosnih sistema OS kao i princip neporečivosti koji je izražen jer ga sam korisnik svojim postupcima dokazuje.
- Loša strana ovakvog sistema što je specijalizovan za svaku aplikaciju
- Tipičan primer je program za E-mail koji koristi PGP model šifrovanja radi obezbeđivanja tajnosti, ili SSL protokol komunikacije između dva sagovornika.
- Primeri ovakvog načina zaštite su SET, S/MIME i PGP protokoli.

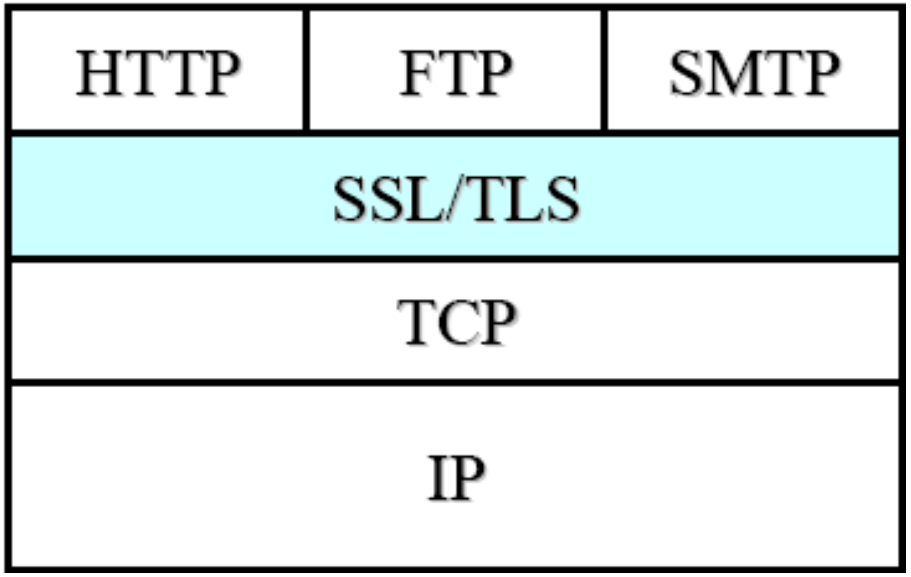


5.2 - Sigurnosne arhitekture

Transportni sloj

- Zaštita se vrši prilikom formiranja segmenata tako da se zaštita obavlja za svaku aktivnost nezavisno od programa što je prednost
- Realizuje se na krajnjim tačkama i zavisna je od korišćenog protokola
- Drugi pristup je da se zaštita implementira iznad transportnog sloja
- Koristi se **TLS** (*Transport Layer Security*) protokol za obezbeđenje provere identiteta, integriteta i poverljivosti.
- Prethodnik ovom protoklu je **SSL**-*Secure Sockets Layer* protokol

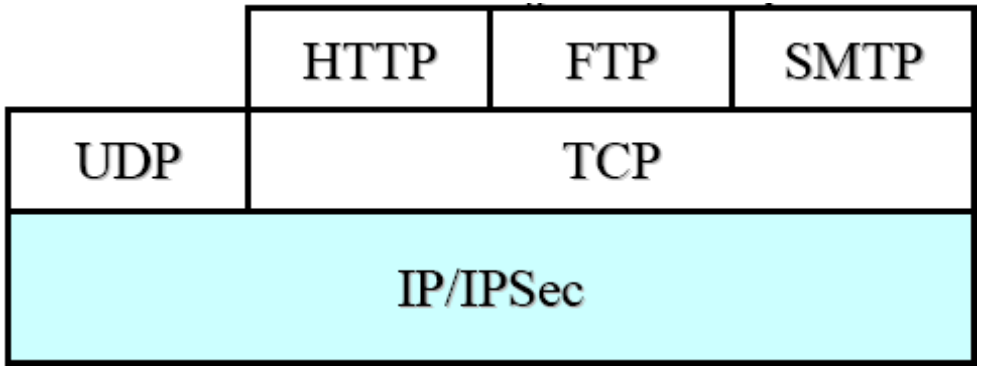
- SSL se nalazi iznad TCP sloja i generalno može se ugraditi kao osnovni protokol transparentan za aplikacijski nivo.
- Međutim, najčešće se ugrađuje kao dodatak klijentskim i serverskim aplikacijama koje koriste TCP na transportnom nivou.



5.2 - Sigurnosne arhitekture

Mrežni sloj

- Ukoliko se odlučimo na implementaciju na ovom sloju imaćemo značajnu prednost u univerzalnosti i nezavisnosti od viših slojeva.
- Sada smo u mogućnosti da formiramo **VPN** (*Virtual Private Network*) i intranet koristeći **IPsec** kao sigurnosni mehanizam.
- Ono što je slaba strana zaštite na ovom nivou je što je praktično nemoguće obezbediti neporecivost zahteva tako da se to ostavlja sloju aplikacije da razreši.
- Jedan od pristupa je da se zaštita implementira iznad IP sloja, ali ispod bilo kog transportnog protokola, kao što je TCP i UDP.
- Postoji više prednosti za implementiranje zaštite na ovom nivou, a osnovna je ta što obezbeđuje siguran prenos na nivou paketa i transparentnost za sve protokole višeg nivoa.



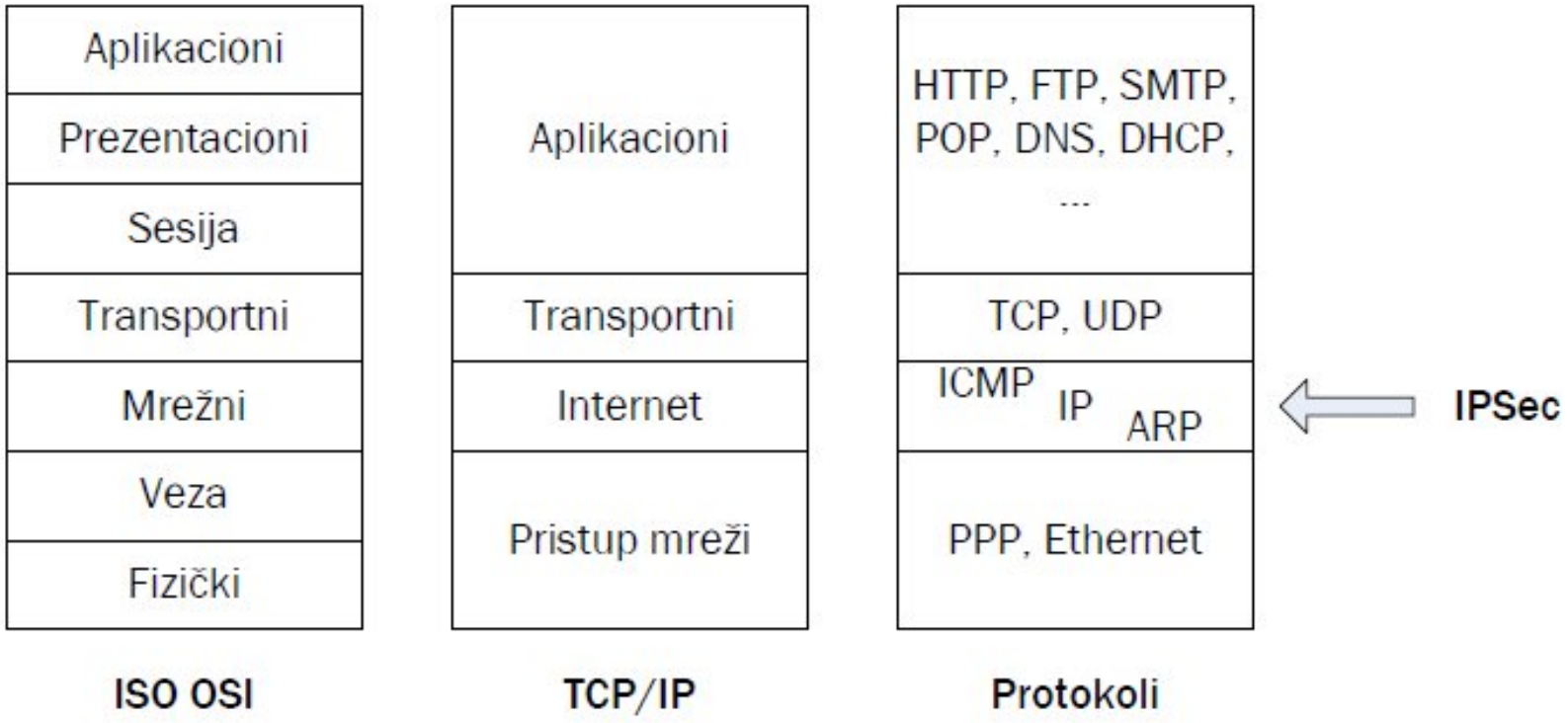
5.2 - Sigurnosne arhitekture

Sloj veze

- Na ovom nivou se štiti sama kombinacija nula i jedinica i to se najčešće realizuje korišćenjem hardverskih uređaja za šifrovanje.
- Prednost ovakvih rešenja je brzina ali samo na tzv. iznajmljenim permanentnim vezama kada su uspostavljene između dve tačke.
- Istovremeno ovaj hardver koji se koristi je i njihova slaba strana jer su kriptografski algoritmi koji se koriste manje jačine kako bi obezbedili potrebnu brzinu u radu.

5.3 – IPsec protokol

- **IPSec**(IP Security), skup proširenja protokola IPv4 koji obezbeđuje osnovne sigurnosne aspekte mrežne komunikacije: privatnost, integritet, proveru identiteta i neporečivost.
- **IPSec** implementira sigurnosne mehanizme mrežne komunikacije na mrežnom sloju OSI referentnog modela, odnosno na Internet sloju skupa protokola TCP/IP.



5.3 – IPsec protokol

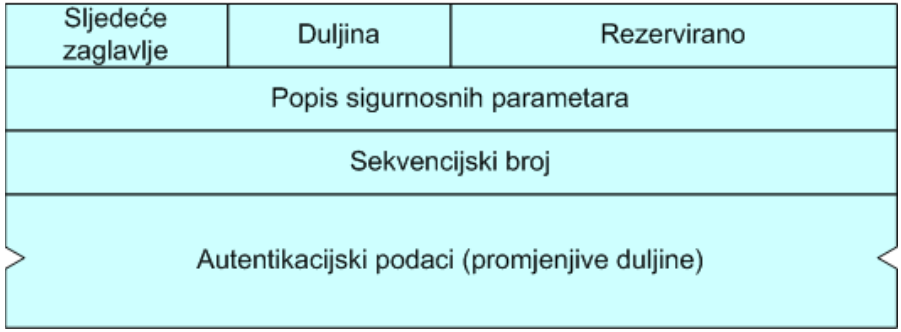
- IPSec definiše informacije koje se moraju dodati IP paketu kako bi se obezbedili privatnost, integritet, provera identiteta i način šifrovanja sadržaja paketa.
- IPSec koristi sledeće protokole i standarde:
  - Diffe-Hellmanov protokol za razmenu ključeva između dva učesnika u komunikaciji,
  - Digitalni potpis,
  - DES, 3DES i AES simetrične algoritme,
  - HMAC (*Hasing Masage Authentication*) - MD5, SHA,
  - Sertifikati.
- Skupom proširenja IPv4 protokola, IPSec osigurava osnovne sigurnosne aspekte mrežne komunikacije: tajnost, integritet, autentifikacija i neporecivost.
- Valja napomenuti da IPSec, osim što proširuje IPv4 koji se trenutno koristi, dolazi i kao integralni deo IPv6 protokola

5.3 – IPsec protokol

- IPSec se implementira korišćenjem dva međusobno nezavisna protokola koji osiguravaju različite aspekte sigurnosti:
- **AH** (*authentication header*) - IP protokol 51 definisan je u RFC 2402 dokumentu i osigurava autentifikaciju, integritet i neporecivost IP datagrama, ali ne može osigurati i tajnost podataka.
- **ESP** (*encapsulated security payload*) – IP protokol 50 definisan je u RFC 2406 dokumentu i može osigurati autentikaciju, integritet, neporecivost i tajnost podataka
- Oba protokola, AH i ESP, modifikuju standardni oblik IP datagrama

5.3 – IPsec protokol – AH

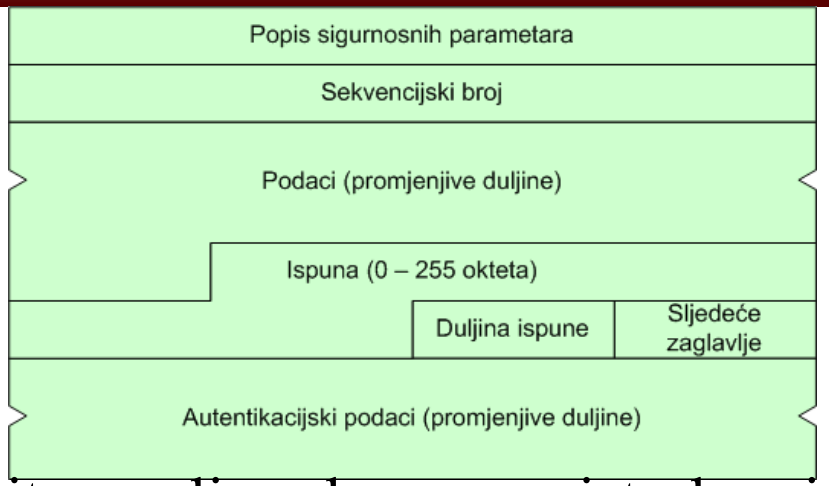
- Protokolom je definisano vlastito (AH) zaglavlje koje se umeće između IP zaglavlja i IP podataka
- AH protokol ne enkapsulira podatke protokola kojima pruža uslugu.



- **Sledeće zaglavlje -** 8-bitno polje koje identifikuje tip podataka koji sledi nakon AH zaglavlja (na primer 6 – TCP, 17 – UDP, 51 – ESP).
- **Dužina -** polje koje specificira dužinu AH zaglavlja. Dužina se računa kao dužina 32-bitnih reči umanjena za vrednost 2.
- **Rezervirano** - polje dužine 16 bita je rezervisano za buduće potrebe.
- **Popis sigurnosnih parametara** - 32-bitno polje koje uz IP adresu i sigurnos.protokol(AH), definiše jedinstveni skup sigurnosn.parametara
- **Sekvencijski broj** - polje dužine 32 bita koje služi za osiguranje od napada ponavljanjem paketa, a povećava se prilikom svakog slanja paketa koji ima identični SA skup sigurnosnih parametara.
- **Autentifikacijski podaci** - polje koje sadrži autentifikacijske podatke (ICV) na osnovu kojih se proverava integritet i autentičnost poruke

5.3 – IPsec protokol - ESP

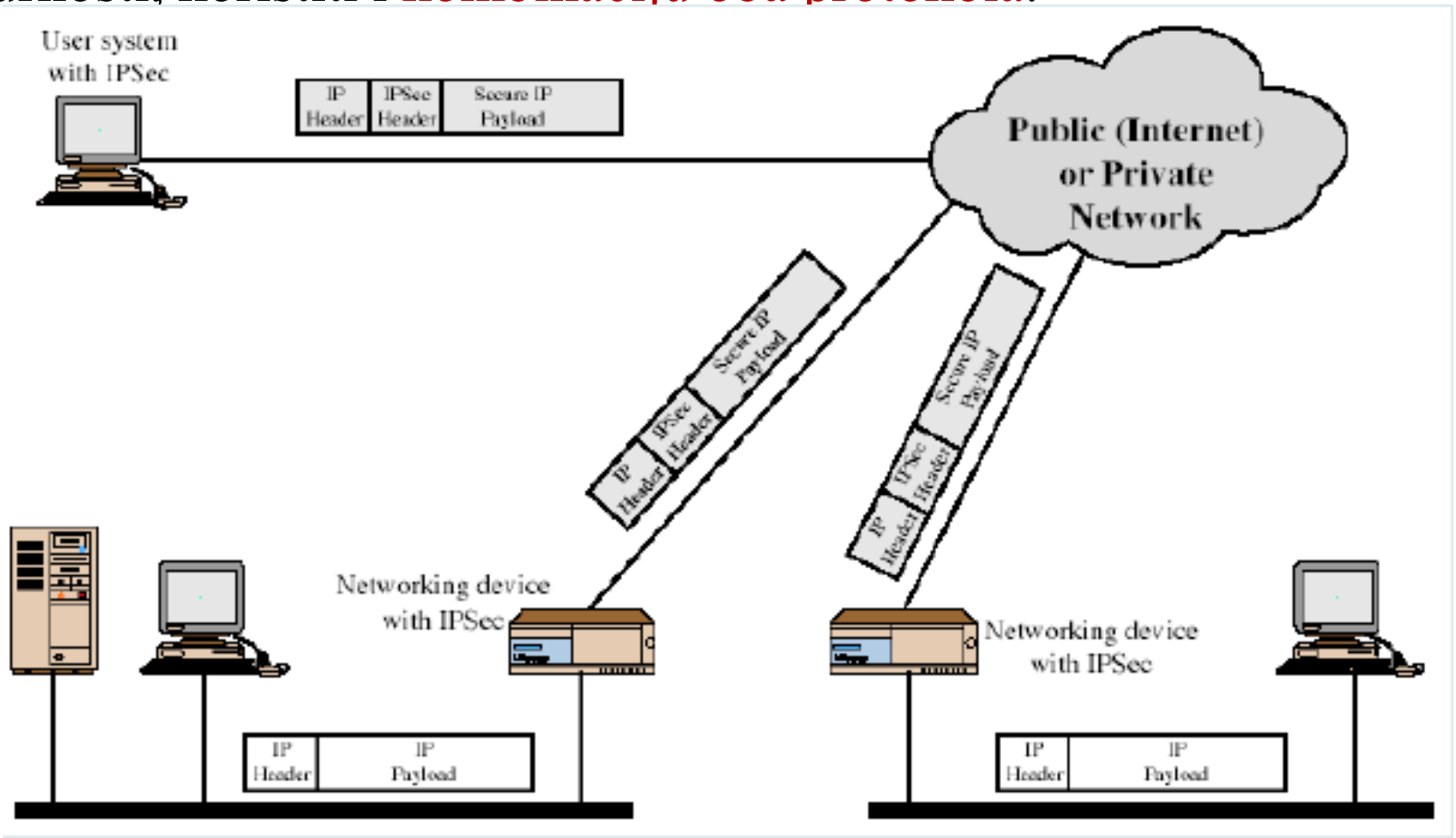
- Ovaj protokol takođe definiše vlastito zaglavlje koje se umeće iza IP zaglavlja, te enkapsulira sve podatke protokola višeg sloja, dodajući pri tom završni slog u kojem mogu biti sadržani autentifikacijski podaci.



- **Popis sigurnosnih parametara** - 32-bitno polje u kome se, isto kao i kod AH, definiše jedinstveni SA skup sigurnosnih parametara
- **Sekvencijski broj -** dužine 32 bita, služi za osiguranje od napada.
- **Podaci i ispuna -** sadrži deo sa podacima IP paketa i ispunu.
- **Dužina ispune** - ovo 8-bitno polje definiše dužinu prethodno korišćene ispune u oktetima. Dozvoljene vrednosti su od 0 do 255.
- **Sledeće zaglavlje -** ponovno kao i kod AH, 8-bitno polje koje identifikuje tip podataka koji sledi nakon ESP zaglavlja.
- **Autentifikacijski podaci -** Ovo polje proizvoljne dužine nije obavezno, a koristi se samo u slučaju da je u SA skupu sigurnosnih parametara specificirana usluga autentifikacije.

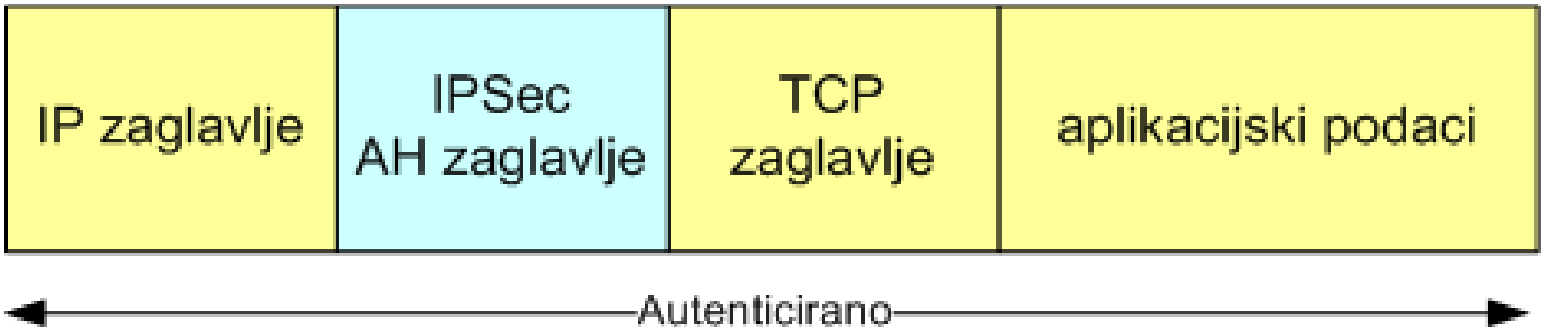
5.3 - IPsec protokol - način rada

- IPSec definiše dva osnovna načina rada: transportni i tunelovanje.
- Oba protokola, AH i ESP, mogu se koristiti u transportnom načinu rada ili za tunelovanje.
- Takođe, moguće je, u slučaju potrebe za dodatnim podizanjem nivoa sigurnosti, koristiti i kombinaciju oba protokola.



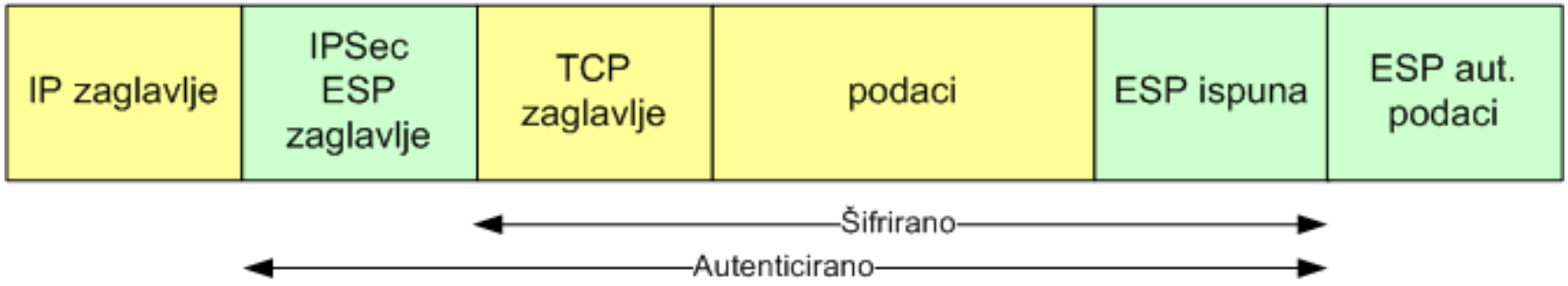
5.3 - IPsec protokol - transportni način

- Transportni način rada namenjen je prvenstveno za uspostavljanje sigurne komunikacije između entiteta, odnosno tzv. host-to-host komunikaciju u privatnim LAN ili WAN mrežama.
- Za transportni način rada nužno je da obe krajnje tačke (izvor i odredište) podržavaju IPSec.
- Korišćenjem AH i ESP protokola moguće je postići različite aspekte sigurne komunikacije.
- **AH** – ukoliko se u transportnom načinu rada koristi AH protokol, moguće je osigurati integritet, autentifikaciju i neporecivost, a AH zaglavlje se dodaje odmah iza IP zaglavlja



5.3 - IPsec protokol-transportni način

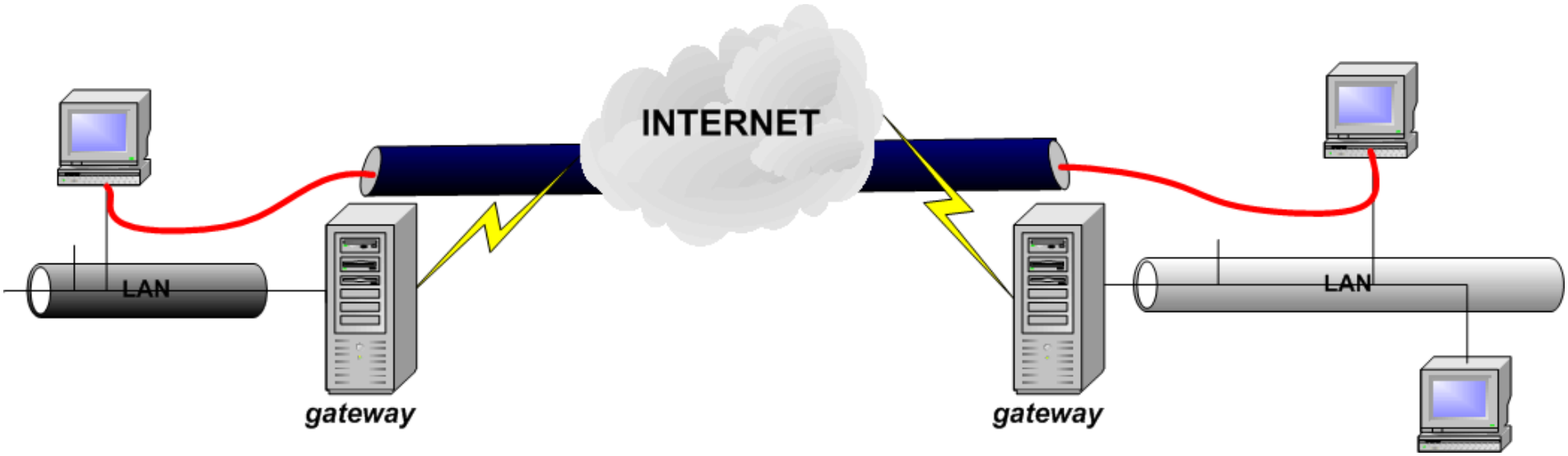
- U transportnom načinu rada ESP osigurava integritet, autentifikaciju, neporecivost i tajnost podataka koji se prenose.
- Ukoliko se za IPSec koristi ESP, polje protokol u IP zaglavlju sadržaće vrednost 50 (ESP) dok je kod AH protokola ta vrednost 51, a polje sledeće zaglavlje u ESP zaglavlju sadržaće vrednost koja odgovara enkapsuliranim podacima iz višeg sloja
- Iza enkapsuliranih podataka ESP takođe dodaje ispunu, te opciono (ukoliko je u SA skupu sigurnosnih parametara specificirana i autentifikacija) polje autentikacijski podaci.



5.3 - IPsec protokol - tunelovanje

- Tunelovanje je drugi način rada ili druga funkcionalnost IPSec
- IPSec služi za uspostavljanje sigurne komunikacije između gateway uređaja na udaljenim mrežama, osiguravajući tako virtualnu privatnu komunikaciju, odnosno uspostavljajući VPN vezu
- Ovde krajnji entiteti u komunikaciji ne moraju podržavati IPSec
- Čitava komunikacija za njih je potpuno transparentna jer sve operacije nužne za sigurnu komunikaciju korišćenjem IPSec-a obavljaju ***gateway***-i
- ***Gateway*** uređaji na udaljenim mrežama predstavljaju ulaznu, odnosno izlaznu tačku sigurnog komunikacionog kanala.
- Oni preko nesigurnog medijuma (Internet) formiraju sigurni tunel,
- Korišćenje tunelskog načina rada takođe je moguće i u host-to-host ili host-to-gateway komunikaciji, no tada ponovo krajnji entiteti ili entitet moraju podržavati IPSec.

5.3 - IPsec protokol - tunelovanje



5.3 - IPsec protokol - tunelovanje

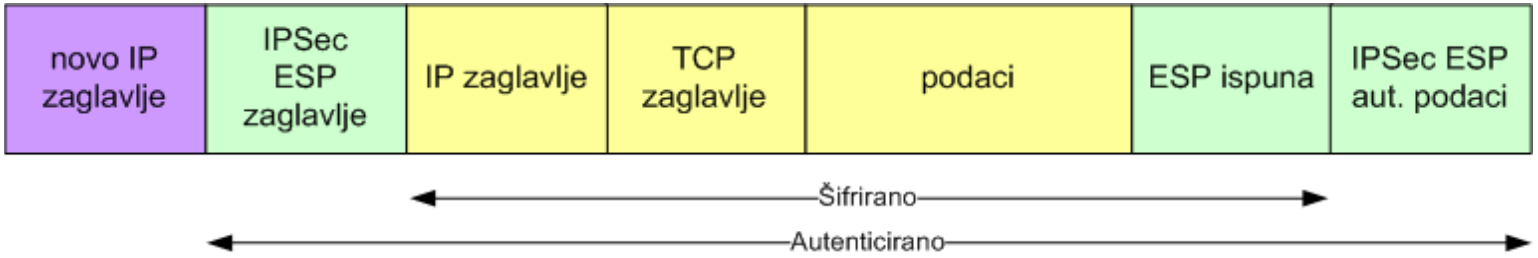
- Za razliku od transportnog načina rada gde se AH odnosno ESP zaglavlja dodaju unutar postojećeg IP datagrama, kod tunelovanja se formira novi IP datagram koji enkapsulira originalni IP datagram

U načelu, komunikacija između dva entiteta funkcioniše na sledeći način:

1. Izvorni računar formira IP datagram i šalje ga preko lokalne mreže lokalnom gateway uređaju.
2. Gateway uređaj enkapsulira čitav originalni IP datagram u novi datagram, te formira odgovarajuća AH odnosno ESP zaglavlja.
3. Tako formirani datagram se šalje preko uspostavljenog tunela do gateway uređaja na udaljenoj mreži koji uklanja dodatna zaglavlja, te po potrebi vrši dešifrovanje i proveru integriteta paketa.
4. Nakon toga originalni IP datagram se isporučuje ciljnom računaru.

5.3 - IPsec protokol - tunelovanje

- **AH** – ukoliko se želi osigurati samo integritet, autentikacija i neporecivost poruka, a tajnost nije obavezna, koristi se AH protokol.
- U tom slučaju originalni IP datagram, koji sadrži adresu krajnjeg odredišta, enkapsulira se u novi IP datagram kome se dodaje odgovarajuće AH zaglavlje
- U ovom slučaju polje protokol novog IP zaglavlja koje sadrži adresu krajnje tačke IPSec tunela ima vrednost 51 (AH), dok polje sledeće zaglavlje unutar AH zaglavlja ima vrednost 4 (enkapsulirani IP).
- **ESP** – ukoliko se osim autentikacije, integriteta i neporecivosti želi osigurati i tajnost komunikacije, nužna je upotreba ESP protokola.
- Ovde se vrši šifrovanje čitavog originalnog IP datagrama, a takođe je osigurana autentifikacija, integritet i neporecivost čitavog datagrama, pošto je sam datagram enkapsuliran u novi IP paket.



5.4 - SSL (Secure Socket Layer)

- Predstavlja protokol koji omogućava siguran kanal između dva uređaja uz mogućnost identifikacije uređaja na drugom kraju.
- SSL je takođe metoda šifrovanja podataka putem transportnog protokola poput TCP-a.
- Razvijen je od strane Netscape-a, 1994.god. SSL verzija 3.0 objavljena je 1996. godine, a njegov naslednik TLS predstavljen je 1999. godine
- Siguran kanal o kojem je ovde reč je transparentan što znači da podaci koji su poslati s jedne strane nepromenjeni stižu do druge strane.
- Ova karakteristika omogućava jednostavnu implementaciju SSL-a u postojeće standarde i protokole
- Prvi zadatak koji je SSL trebalo da ispuni je ***poverljivost***.
- Autentifikacija – korisnik je morao biti siguran da komunicira s onim serverom s kojim želi ostvariti komunikaciju, a ne nekim trećim
- Druga karakteristika je ***spontanost***.To znači da korisnik može spontano izabrati WEB server s kojim želi izvršiti određenu transakciju tj. poslovati s onim s kim do tada nije imao nikakvog poslovnog iskustva
- Treći cilj i zadatak je bio **povezati SSL sa HTTP-om**

5.4 - SSL (Secure Socket Layer)

Implementacijom SSL protokola postižu se sledeći ciljevi:

- **Kriptografska zaštita** -obezbeđuje mehanizme za šifrovanje podataka.
- **Nezavisnost od softvera i hardvera -** programeri pišu softver u kome je implementiran SSL tako da dva različita programa, na primer, Web server i čitač Weba mogu razmenjivati parametre šifrovanja, a da pritom ne poznaju kod onog drugog.
- **Proširivost** - mogućnost u slučaju potrebe uklopiti novi simetrični algoritmi i algoritmi s javnim ključem. Čime se izbegava potreba za projektovanje novih protokola.
- **Efikasnost** - SSL pamti(kešira) komunikacione parametre ostvarenih veza kako bi smanjio broj veza koje mora ponovo da uspostavlja, čime manje opterećuje procesor, a ujedno i mrežu.

5.4 - SSL (Secure Socket Layer)

Tri osnovna svojstva SSL protokola su:

- **Privatnost** - šifrovanje se vrši simetričnim algoritmom(DES i RC4).
- **Mogućnost provere identiteta** - indentitet klijenata, odnosno servera, može se proveriti javnim ključem. SSL koristi RSA i DSS kao algoritme s javnim ključevima.
- **Pouzdanost** - proverava se integritet primljenih podataka. SSL koristi SHA i MD5 heš funkcije.

Dakle, SSL protokol obezbeđuje:

1. šifrovanje podataka,
2. autentifikaciju i
3. kontrolu integriteta poruke.

5.4 - SSL (Secure Socket Layer)

- Namena SSL protokola je da obezbedi sigurnu (zaštićenu) vezu s kraja na kraj koristeći usluge transportnog TCP sloja.
- Ovaj protokol definiše dva pojma: **pojam sesije** i **pojam konekcije**.

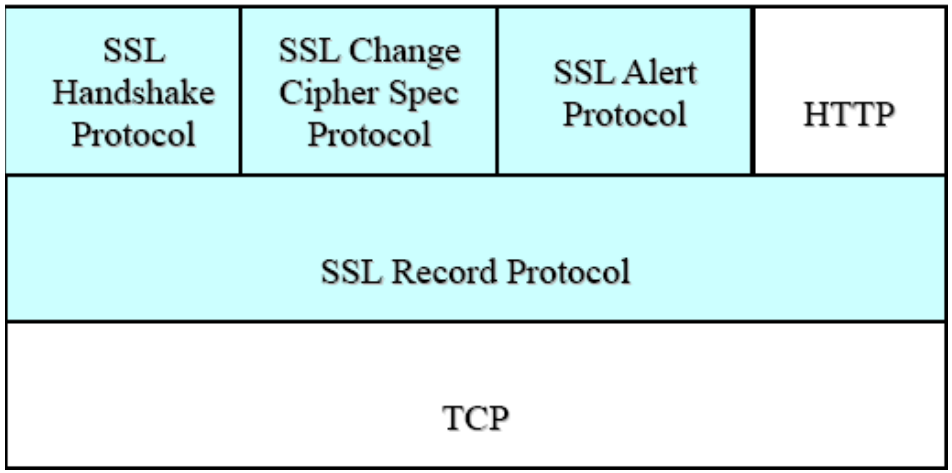
Konekcija *podrazumeva transport podataka.*

- Svaka konekcija je pridružena nekoj sesiji a definisana je sa:
  1. četiri simetrična ključa: jedan za potpisivanje i jedan za šifrovanje podataka za obe strane u komunikaciji,
  2. inicijalizacionim vektorom,
  3. serverskim i klijentskim slučajnim brojem
  4. sekvencijskim brojem.

Sesija *je dogovor između klijenta i servera koji obezbeđuju sigurnu vezu i može se koristiti u više konekcija.*

- Sesija je definisana sa sledećim parametrima:
  1. brojem sesije,
  2. sertifikatima,
  3. metodom kompresije,
  4. kriptografskim algoritmima
  5. tajnim podacima za generisanje simetričnih ključeva.

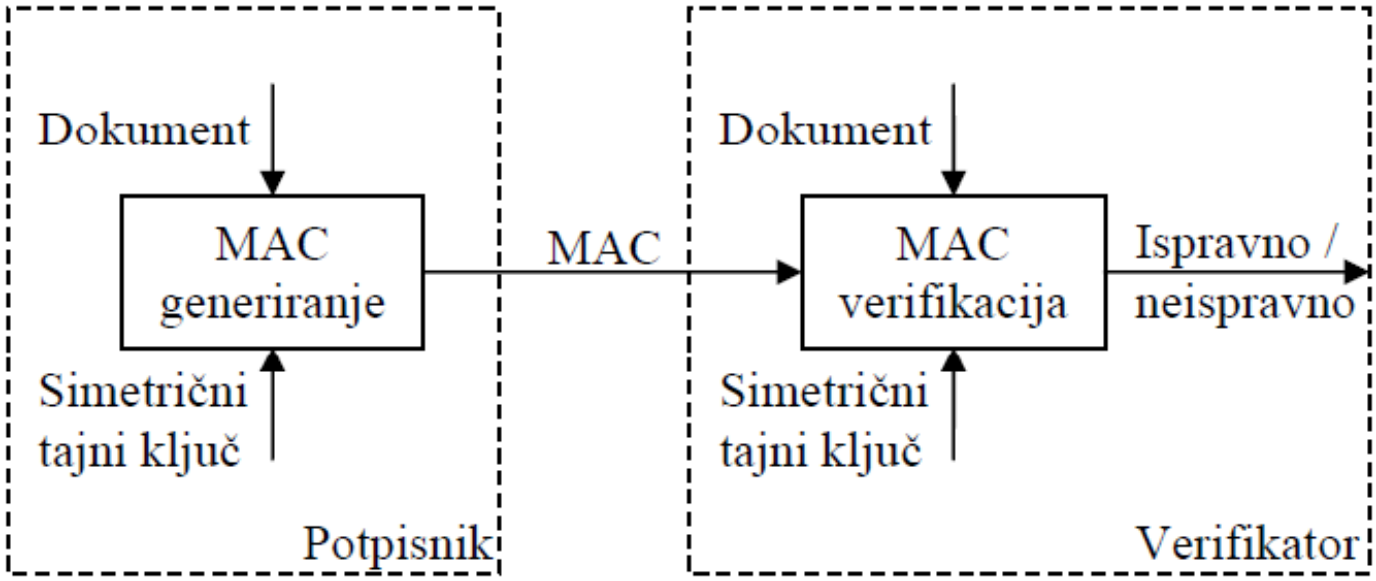
5.4 - SSL (Secure Socket Layer)



- SSL Record Protocol se brine o šifrovanju/dešifrovanju informacija koje se prenose i tu uslugu pruža višim slojevima.
- U praksi to je obično HTTP preko koga Web čitači i serveri razmenjuju podatke.
- Tri viša protokola: protokol za dogovaranje/uspostavljanje veze (SSL Handshake Protocol), protokol za promenu ključa (SSL Change Cipher Spec Protocol), i protokol za upozorenje (SSL Alert Protocol) služe za uspostavljanje veze, prelazak u režim šifrovanja simetričnim ključem i nadgledanje veze.

5.4 - SSL (Secure Socket Layer)

- SSL rekord protokol na predajnoj strani prihvata podatke od aplikacijskog sloja, vrši njihovu fragmentaciju u blokove, opciono komprimuje podatke, dodaje autentifikaciju (MAC – message authentication code), šifruje podatke, dodaje zaglavlje i predaje TCP sloju radi slanja.
- Na prijemnoj strani podaci se preuzimaju od TCP sloja, dešifruju, izračunava se i poredi MAC radi provere ispravnosti, vrši dekompresija podataka, defragmentacija, i na kraju podaci se predaju aplikacijskom nivou.



Hvala na pažnji !!!

Pitanja

? ? ?