Preddiplomski studij

Računarstvo

Komunikacijske mreže

12.

Osnove sigurnosti mreža, usluga i aplikacija – sigurnost u Internetu

Ak.g. 2014./2015.

12.1.2015.

slobodno smijete:

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo

pod sljedećim uvjetima:

- **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencijske uvjete ovog djela. Najbolji način da to učinite je poveznicom na ovu internetsku stranicu.
Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.
Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Sadržaj predavanja

- Pojam sigurnosti i sigurnosni zahtjevi
- Pojam ranjivosti i prijetnje
- Komunikacijska sigurnost
- Načini postizanja sigurnosti, tehničke kontrole
- Osnovne kriptografije i njena primjena u komunikacijskim mrežama
- Komunikacijska sigurnost na Internetu
- Sigurnost sustava i vatrozid

Što je *sigurnost*?

- Primjeri nekih izjava koje uključuju pojam „sigurnost”
  - Lozinke su sigurne
    - Moraju biti poznate samo ovlaštenom sustavu ili osobi te ne smiju biti neovlašteno mijenjani
  - Web stranice tvrtke su sigurne
    - Smiju biti poznate bilo kome ali ne smiju biti ne ovlašteno mijenjane
  - Poslužitelj je siguran
    - Na poslužitelju smiju raditi samo ovlaštene osobe, ne smiju se koristiti neovlaštene aplikacije, ne smije biti neovlaštenih izmjena i mora biti na raspolaganju korisnicima
  - Tvrtka je sigurna
    - Svi njeni sustavi su sigurni i na raspolaganju korisnicima
- Iz prethodnih izjava je jasno kako je pojam sigurnosti složen te da ovisi o kontekstu u kojemu se upotrebljava

Definicija pojma *sigurnost*

Sigurnost (engl. *security*)

- Sposobnost mreža, sustava, usluga i aplikacija da se suprotstave neočekivanim slučajnim događajima i zlonamjernim aktivnostima koje mogu narušiti i kompromitirati raspoloživost, vjerodostojnost, cjelovitost i povjerljivost informacije i komunikacije

Sigurnosni zahtjevi (1)

- **Tri temeljna zahtjeva, tzv. CIA trojka**
- **povjerljivost** (engl. *confidentiality*), **tajnost** (engl. *secrecy*)
  - razmijenjene poruke trebaju biti razumljive samo pošiljatelju i namjeravanom primatelju; zaštita komunikacije ili pohranjenih informacija od uvida neovlaštenim korisnicima
- **cjelovitost, integritet** (engl. *integrity*)
  - jamstvo da su informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
- **raspoloživost** (engl. *availability*)
  - informacije moraju biti raspoložive, a sustavi i usluge u operativnom stanju, usprkos mogućim neočekivanim i nepredvidljivim događajima, primjerice nestanku struje, prirodnim nepogodama, nesrećama i zlonamjernim napadima

Sigurnosni zahtjevi (2)

- **U skup mogućih zahtjeva dodaju se još autentičnost i neporecivost**
  - Međutim nisu toliko prihvaćeni kao prethodna tri
- **autentičnost** (engl. *authenticity*)
  - potvrda identiteta korisnika; ovjera vjerodostojnosti (autentifikacija) sudionika komunikacije
- **neporecivost** (engl. *nonrepudiation*)
  - sudionici ne mogu poreći akciju u kojoj su sudjelovali, npr. nemogućnost naknadnog odricanja odaslane poruke

Prijetnje i ranjivosti

- Da bi se desio incident moraju postojati dva preduvjeta: ranjivost i prijenja
- *Ranjivost* (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.
  - Pogreške u programskoj podršci (engl. bugs), propusti u protokolima, kriva upotreba programske podrške ili nekog sustava
- *Prijetnja* (engl. threat) je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu.
  - Izvori prijetnji su ljudski (napadači) ili prirodni (potres, nestanak struje);
  - Dodatno ljudski izvori mogu biti namjerni (napadači) ili slučajni (nepažnja osobe)

Komunikacijska sigurnost

- U nastavku ćemo pogledati prijetnje koje mogu narušiti sigurnost informacija koje razmjenjuju dva čvora, A i B
  - Alternativno ćemo govoriti „sigurnost komunikacije” pod čim se podrazumijeva sigurnost informacije koju razmjenjuju A i B
- Pretpostavljamo da moraju biti ispunjeni svi sigurnosni zahtjevi na informacije/podataka koji se razmjenjuju između A i B kako bi se te informacije smatrale sigurnima(!)
  - Svi zahtjevi su: tajnost, raspoloživost, cjelovitost, autentičnost i neporecivost
  - U određenim slučajevima neće biti potrebno zadovoljiti sve zahtjeve, ali onda neke od prijetnji više ne postoje!
- Za sada pretpostavljamo da se nismo posebno zaštitili!

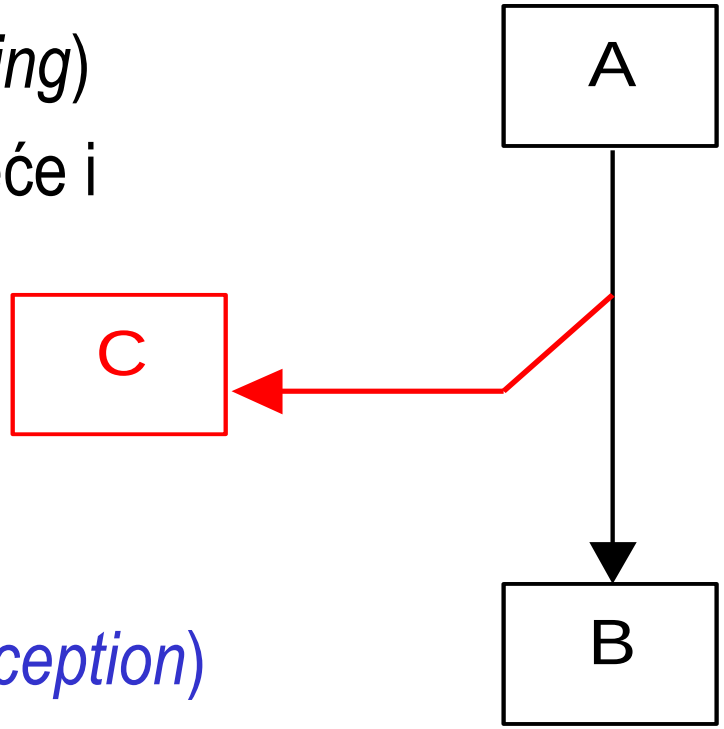
Sigurnosne prijetnje: presretanje, prisluškivanje

Presretanje (engl. *interception*)

Prisluškivanje (engl. *evesdropping*)

Prisluškivanje na vodu (engl. *wiretapping*)

- elektronička komunikacija se presreće i preuzima informacija
- Potencijalne štete
  - Neovlaštena uporaba podataka
  - Potencijalno narušavanje privatnosti



Zakonski regulirano (engl. *lawfull interception*)

Koji sigurnosni zahtjev je narušen?

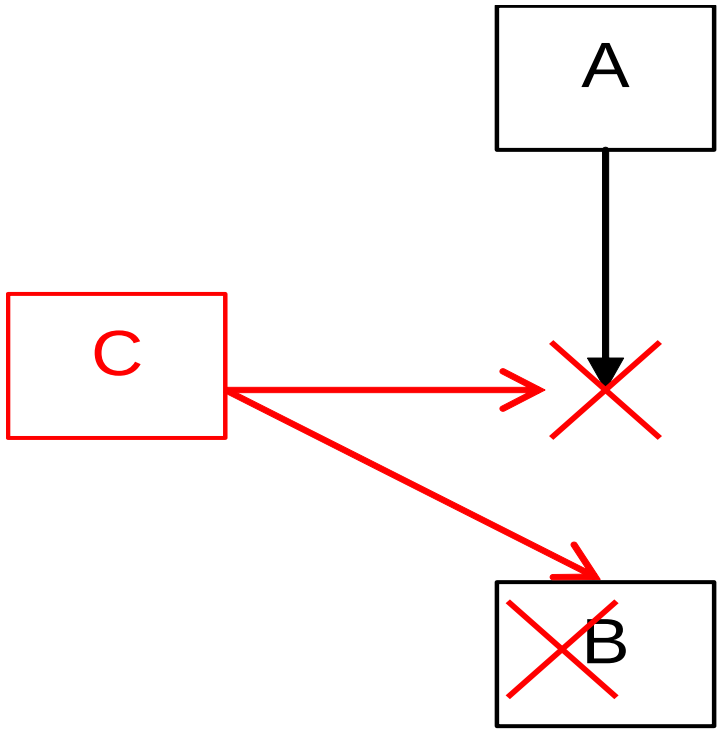
Sigurnosne prijetnje: prekidanje, uskraćivanje

Prekidanje (engl. *interruption*)

- prekidanje normalnog tijeka komunikacije, usluge ili aplikacije

Uskraćivanje usluge (engl. *denial of service*)

- onemogućavanje usluge izazivanjem preopterećenja mreže ili umreženog sustava

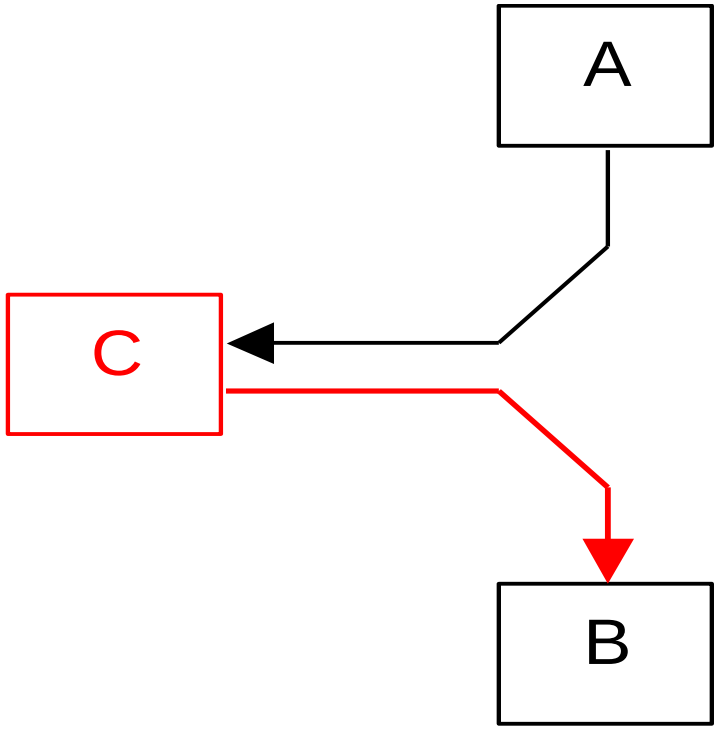


Koji sigurnosni zahtjev je narušen?

Sigurnosne prijetnje: promjena, kašnjenje

Promjena (engl. *modification, tampering*)

- promjena ili uništenje informacije
- kašnjenje može izazvati isti učinak – informacija postaje nevažna



- Ova forma napada još se zove „čovjek u sredini” (engl. man in the middle, MITM)

Koji sigurnosni zahtjevi su narušeni u ovom slučaju?

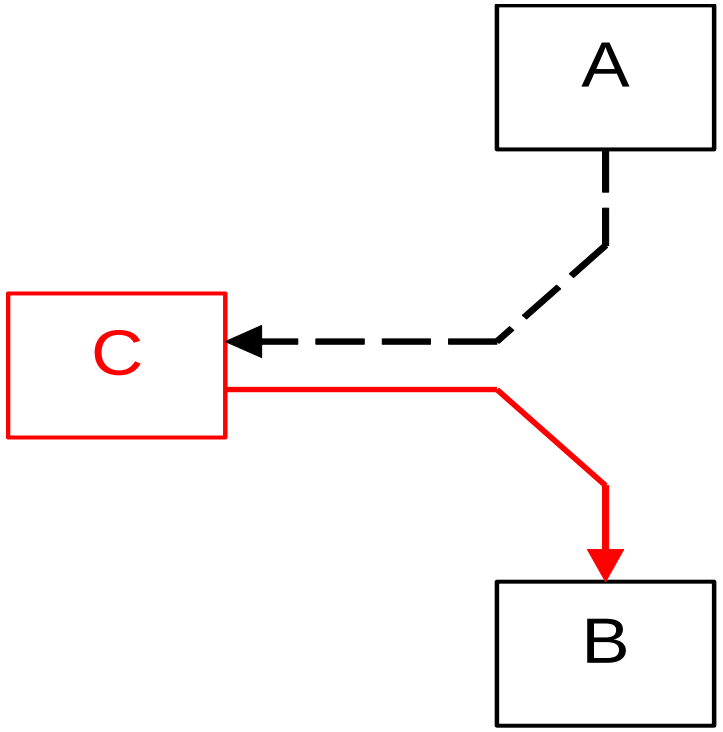
Sigurnosne prijetnje: fabrikacija, ponavljanje

Fabrikacija (engl. *fabrication*)

- ubacivanje zlonamjerne informacije

Ponavljanje (engl. *replay*)

- ubacivanje informacije prethodno preuzete presretanjem



Koji sigurnosni zahtjevi su narušeni u ovom slučaju?

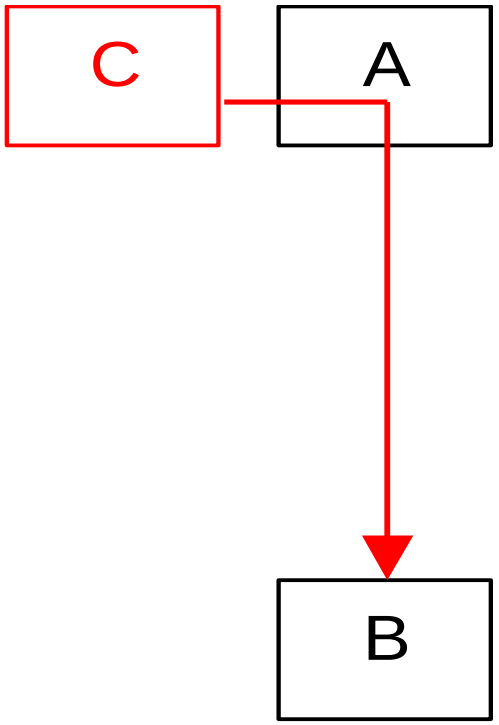
Sigurnosne prijetnje: lažno predstavljanje

Lažno predstavljanje

maskiranje (engl. *masquerade*)
utjelovljenje (engl. *impersonation*)

- preuzimanje identiteta i uloge korisnika

Koji sigurnosni zahtjevi su narušeni u ovom slučaju?



Sigurnosne prijetnje: „Čovjek u sredini”

- Često se u kontekstu komunikacija govori o napadu „čovjek u sredini”
  - engl. Man in the Middle, MITM
- To je situacija u kojoj su prisutne sve prethodno spomenute prijetnje
  - Kako bi sve navedene prijetnje bile ostvarive napadač se mora nalaziti negdje na putu kojim se prenose podaci

Ranjivosti u komunikacijskim sustavima

- U komunikacijskim sustavima ranjivosti se mogu pojaviti u protokolima, njihovim implementacijama i krajnjim sustavima
- Ranjivosti u protokolima
  - Dosta protokola Interneta je nastalo u vrijeme kada sigurnost nije bila visoko na listi prioriteta
  - Primjeri ranjivih protokola: ARP, Ethernet, IP, TCP, UDP, niz aplikacijskih protokola
  - Navedeni protokoli su ranjivi jer nemaju mehanizama uz pomoć kojih bi se jamčilo očuvanje sigurnosnih zahtjeva
- Krajnjim sustavima
  - Krajnji sustavi mogu imati pogreške u implementaciji, konfiguraciji ili neadekvatne operativne procedure

Načini na koje postižemo sigurnost

- Pojedinu zaštitu koju primjenjujemo kako bi postigli sigurnost nazivamo **kontrola** (engl. control)
- Sve kontrole su razvrstane u tri velike grupe:
  - Fizičke kontrole
    - Kamere, zaštitari, blindirana vrata, …
  - Tehničke kontrole
    - Kriptografija, vatrozidi, sustavi za detekciju napada, …
  - Administrativne kontrole
    - Politike, pravilnici, itd.
    - Različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašati, kako uređaji moraju biti podešeni, …
- U kontekstu predmeta Komunikacijske mreže interesiraju nas tehničke kontrole

Tehničke kontrole

- **Osnove** kriptografije
  - Intenzivno se koristi u komunikacijskoj sigurnosti
  - Mi ćemo proći kroz mali dio kriptografije, nužan za razumijevanje drugih tema u ovim predavanjima
- Infrastruktura javnog ključa (PKI)
- Protokoli na Internetu za zaštitu komunikacije
- Sigurnost Weba i elektroničke pošte
- Vatrozid
- U nastavku ćemo upotrebljavati i izraz *sigurnosni mehanizmi*

Osnovno o kriptografiji i primjeni u komunikacijskim mrežama

Kriptologija, kriptografija i kriptoanaliza

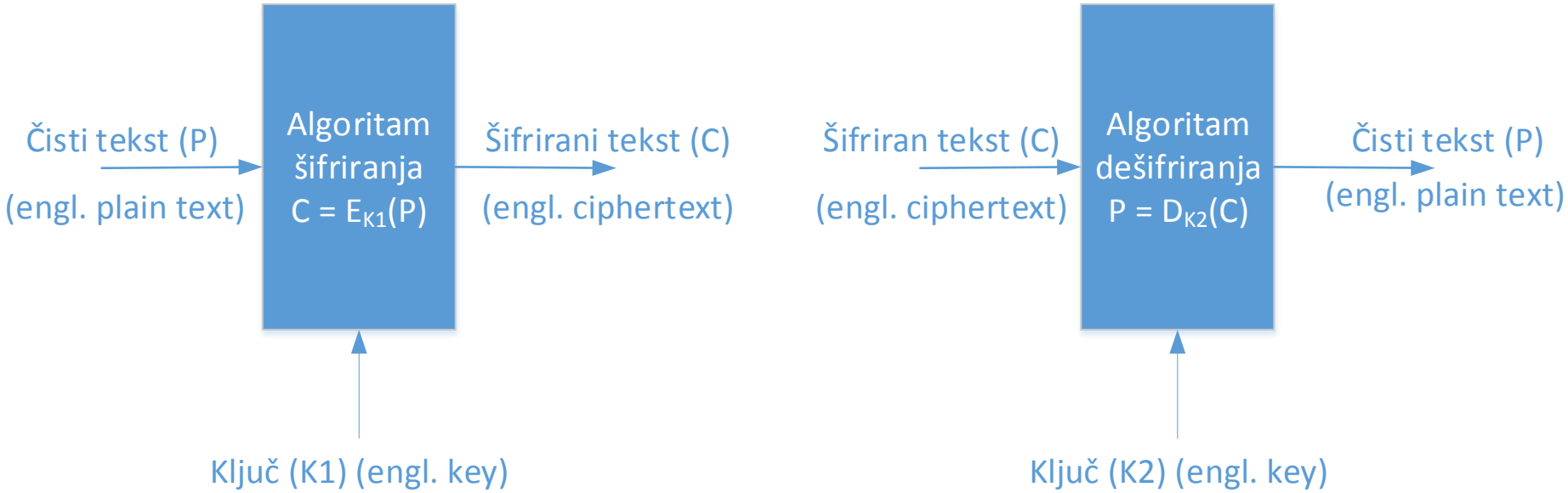
- kriptologija (engl. *cryptology*): znanost koja obuhvaća dvije komplementarne discipline:
  - kriptografija (engl. *cryptography*), kriptografi:
    grana primijenjene matematike koja se bavi transformacijama čija zadaća je pretvaranje podataka u oblik nečitljiv neovlaštenim osobama, sprečavanje neovlaštenih promjena podataka te neovlaštenog korištenja.
  - kriptoanaliza (engl. *cryptoanalysis*), kriptoanalitičari:
    grana primijenjene matematike koja pokušava zaobići zaštite koje smišljaju kriptografi
- U nastavku predavanja bavit ćemo se samo kriptografijom

Kriptografski mehanizmi i njihova primjena

- Osnovni kriptografski algoritmi
  - Simetrično i asimetrično šifriranje i dešifriranje
  - Izračunavanje sažetka poruke
- Primjena osnovnih kriptografskih algoritama
  - Digitalni potpis
  - Osiguranje autentičnosti poruka
- Problem distribucije javnog ključa
  - Raspodijeljeni način distribucije javnih ključeva
  - Infrastruktura javnog ključa

Šifriranje i dešifriranje

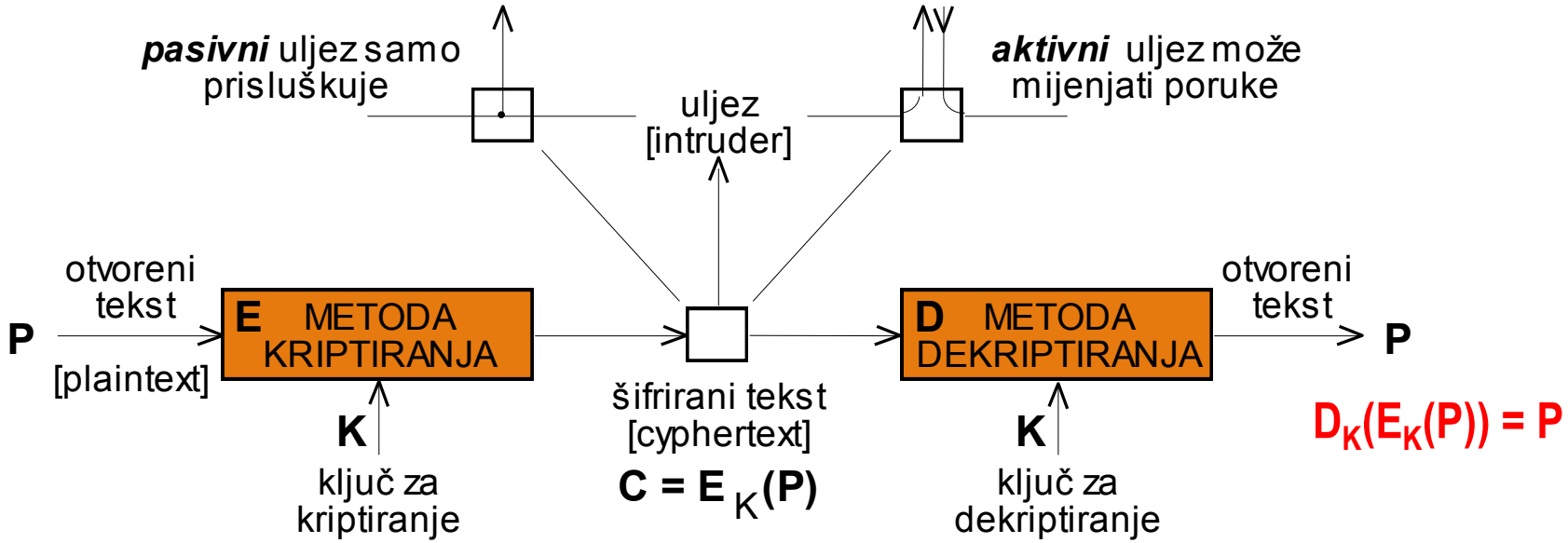
- Zadaća šifriranja je pretvoriti čisti tekst u šifrirani tekst.
- Zadaća dešifriranja je pretvoriti šifrirani tekst u čisti tekst.



- Postoji niz različitih algoritama šifriranja, a o njima ovise svi ostali parametri
  - Svi algoritmi se mogu svrstati u dvije osnovne vrste: simetrične i asimetrične algoritme

Upotreba kriptiranja u komunikaciji

- Prije slanja podataka na komunikacijski kanal podaci se šifriraju, po primitku se dešifriraju
  - Napadač djeluje na komunikacijskom kanalu i pretpostavljamo da može djelovati pasivno I aktivno
  - Cilj je spriječiti napadača u njegovom djelovanju!

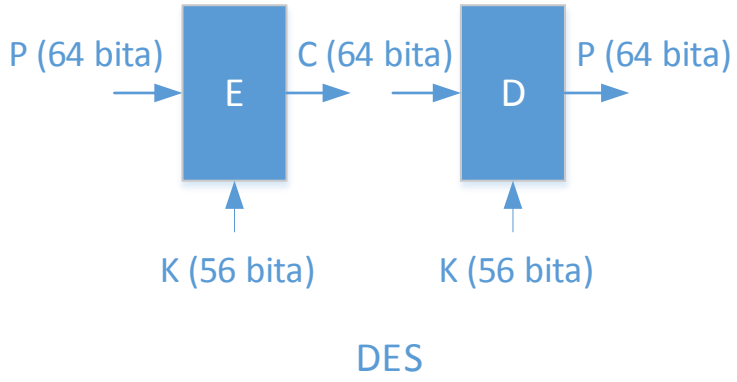


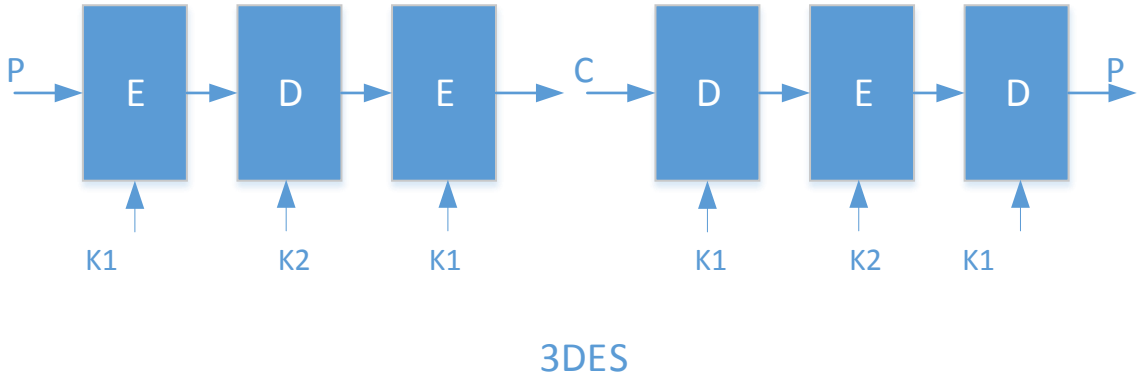
Simetrični algoritmi šifriranja

- **Isti ključ se koristi za šifriranje i za dešifriranje!**
- Algoritmi za šifriranje i dešifriranje su javno poznati
  - Tajnost se temelji na tajnosti ključa!
  - Snaga algoritma se **obično** mjeri duljinom ključa
  - Algoritam mora biti takav da se na temelju poznatog P i C ne može utvrditi ključ!
- Dvije osnovne klase algoritama
  - Blok orijentirani (engl. block ciphers)
    - Ključ je fiksne duljine (56 bita, 64 bita, 128 bita, 192 bita, …)
  - Bit/bajt orijentirani (engl. stream ciphers)
    - Ključ je veličine poruke
- Mnoštvo algoritama, mi ćemo upoznati samo dva, DES i AES

Simetrični blokovski algoritmi šifriranja (1)

- DES (engl. Data Encryption Standard, 1977. godina)
  - Blok je veličine 64 bita, ključ je duljine 56 bita
  - Za današnje pojmove potpuno nesiguran algoritam, grubom silom moguće vrlo brzo otkriti ključ
  - Postoji poboljšanje u vidu ulančavanja više šifriranja (3DES, 1979. godina) čime se postiže duljina ključa od 112 bita, međutim, i dalje nije dovoljno sigurno





Simetrični blokovski algoritmi šifriranja (2)

- AES (engl. Advanced Encryption Standard, 2001. godina)
  - Blok je veličine 128 bita
  - Ključ je duljine 128, 192 ili 256 bita
    - Oznake AES128, AES192, AES256
  - Moderan kriptografski algoritam čija upotreba je sigurna
  - Razvijan tijekom 5 godina na javnom natječaju u kojemu se natjecalo više različitih algoritama
  - javni i nediskriminatorno licencirani algoritam
  - Jedan od uvjeta natječaja bio je i efikasna sklopovska implementacija
    - Moderni procesori sadrže instrukcije koje ubrzavaju šifriranje i dešifriranje korištenjem algoritma AES.

Neki problemi simetrične kriptografije

- Rijetko se šalje točno 64 ili 128 bita
  - Vrlo velika posljedica na **način korištenja** temeljnih algoritama. Neispravnim (naivnim) korištenjem ne postiže se tajnost!
  - Često količina podatak nije višekratnik veličine bloka! I na to treba paziti da se ne omogući napadaču otkrivanje čistog teksta ili ključa
- Odabir i distribucija ključa
  - Ključ mora biti slučajan! Ako nije, napadač bi mogao pogoditi ključ!
  - Kako sigurno distribuirati ključ drugoj strani?!
- Od aktivnog napadača nismo zaštićeni jer nema načina da se utvrdi namjerna modifikacija ili fabrikacija kriptiranog teksta
  - Moraju se uvesti dodatni mehanizmi za tu potrebu (o čemu ćemo malo kasnije)

Asimetrična kriptografija javnog ključa (1)

Kriptografija javnog ključa (engl. *public key cryptography*)

- Algoritmi osmišljeni krajem 70-tih godina prošlog stoljeća
  - Temelje se na teško izračunljivim matematičkim problemima
- Svaki sudionik ima dva ključa: javni ključ i tajni privatni ključ
- Sudionik **objavljuje** jedan ključ koji se zato naziva **javnim ključem** te koji se kombinira s tajnim privatnim ključem:
  - kriptiranje i dekriptiranje s različitim ključevima ~ *asimetrični* postupak
  - E: algoritam kriptiranja, s *javnim ključem* E(P)
  - D: algoritam dekriptiranja, s *privatnim ključem* D(E(P)) = P
  - izrazito teško izvesti D iz E, a E se ne može probiti metodom odabranog otvorenog teksta

Asimetrična kriptografija javnog ključa (2)

Postupak kriptiranja i dekriptiranja:

1. svaki sudionik, A i B, objavljuje svoj javni ključ, E_A i E_B :

   $A \sim E_A$, $B \sim E_B$

2. kriptiranje:

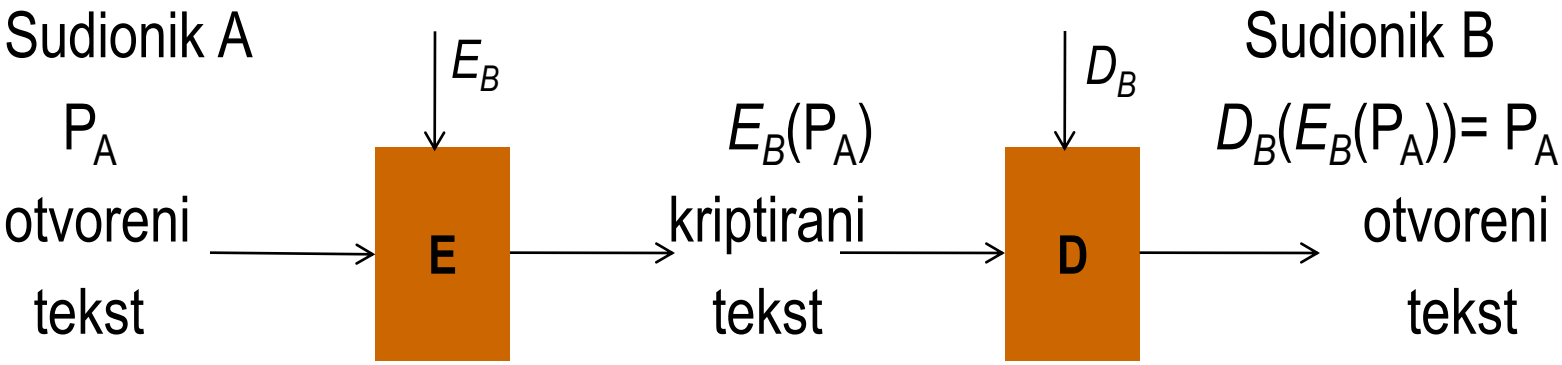
   $A \rightarrow B$: $E_B(P_A)$ javni ključ E_B

   $B \rightarrow A$: $E_A(P_B)$ javni ključ E_A

3. dekriptiranje:

   B: $D_B(E_B(P_A)) \equiv P_A$ privatni ključ D_B

   A: $D_A(E_A(P_B)) \equiv P_B$ privatni ključ D_A



Algoritam RSA

Algoritam RSA (Rivest, Shamir, Adleman; MIT, 1978)

- asimetrični algoritam temeljen na faktorizaciji velikih brojeva:
  - vrlo snažan i siguran algoritam za šifriranje i digitalno potpisivanje
  - zasniva se na teoriji brojeva:
    nalaženje prim-brojeva ($> 10^{100}$) prilikom faktorizacije velikih brojeva
  - sigurnost zasnovana na vrlo velikom vremenu potrebnom za faktorizaciju, npr. za 200-znamenkasti broj oko $4 \cdot 10^9$ godina na računalu s $t_{instr} = 1\ \mu s$
  - glavni nedostatak: za dobru sigurnost potrebni *dugi* ključevi (≥ 1024 bita), tako da je izračunavanje dosta sporo
- opći nedostatak asimetričnih algoritama: sporost, pogotovo kod velikih količina podataka (100 - 1000 puta sporiji od simetričnih)

Šifriranje u praksi

- Simetrični algoritmi šifriranja brzi, ali je problem kako distribuirati ključeve
- Asimetrični algoritmi imaju *manje problema* s razmjenom ključeva, ali su spori
- Za razmjenu ključeva koriste se asimetrični algoritmi, a za samo šifriranje simetrični
  - **U načelu** postupak je sljedeći: jedna strana generira slučajan broj, simetrični (sjedničkі) ključ, te ga šifrira javnim ključem primatelja. Potom to šalje primatelju koji dešifrira simetrični ključ korištenjem svog privatnog ključa
    - Još uvijek imamo probleme o kojima ćemo nešto kasnije
  - Za razmjenu ključeva mogu se koristiti i posebni protokoli koji služe samo tome, kao što je primjerice Diffie-Hellman

Kriptografske funkcije sažetka

Sažetak poruke (engl. *message digest/hash,* MD)

- jednosmjerna funkcija, MD, koja iz proizvoljno dugog teksta P generira niz bita fiksne duljine, sa sljedećim svojstvima
  - lako izračunati MD(P)
  - nemoguće izračunati P iz MD(P)
  - za dani P nemoguće izračunati P' ~ MD(P') = MD(P)
- Neke često korištene funkcije i duljina sažetka
  - SHA2 (varijante SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - SHA3 (varijante SHA3-224, SHA3-256, SHA3-384, SHA3-512)
- Funkcije sažetka koje se više ne preporuča koristiti
  - MD5 (1992, 128 bita), SHA-1 (1995, 128 bita)

Jedna jednostavna primjena funkcija sažetka

- Prilikom skidanja datoteka s poslužitelja na Internetu sprečavanje pogrešaka i/ili namjernih malicioznih izmjena
  - Na poslužitelju se nalazi datoteka koju želimo skinuti i njen sažetak (jedan ili više, izračunati različitim funkcijama)
  - Nakon dohvata datoteke i sažetka, izračunavamo ponovo sažetak datoteke i uspoređujemo ga s onim skinutim s Interneta
  - Za izračunavanje sažetka postoje već gotovi programi za sve operacijske sustave
    - Na Linux OS-u: md5sum, sha1sum, sha256sum, sha512sum
- Navedeni način promjene ima problem! Koji? I kako ga riješiti?

Digitalni potpis (1)

- Problem iz prethodnog primjera možemo riješiti korištenjem digitalnog potpisa
  - zamjena za vlastoručne potpise u porukama
- Sustav koji podržava sljedeće zahtjeve:
  - primatelj može provjeriti identitet pošiljatelja
    ~ ovjera pošiljatelja
  - pošiljatelj ne može kasnije poreći sadržaj poruke
    ~ neporecivost poruke
  - primatelj nije mogao “izmisliti” poruku

Digitalni potpis (2)

- Za potpisivanje koristimo kriptografiju javnog ključa
  - Mora biti zadovoljen uvjet da je E(D(P)) = P što RSA zadovoljava
    - Treba primjetiti da je u takvim sustavima svejedno koji je javni a koji tajni ključ!
- Postupak generiranja potpisa
  - Pošiljatelj poruke izračunava sažetak MD(P) poruke P
  - Sažetak poruke kriptira svojim **tajnim ključem** $D_A(MD(P))$
    - To je digitalni potpis!
- Postupak provjere potpisa
  - Pošiljatelj dekriptira kriptirani sažetak, $E_A(D_A(MD(P)) = MD(P)$
  - Zatim izračunava sažetak primljene poruke MD(P')
  - Ako su oba sažetka ista, tada poruka nije mijenjana te ju je mogao potpisati samo A

Osiguranje autentičnosti i cjelovitosti poruka

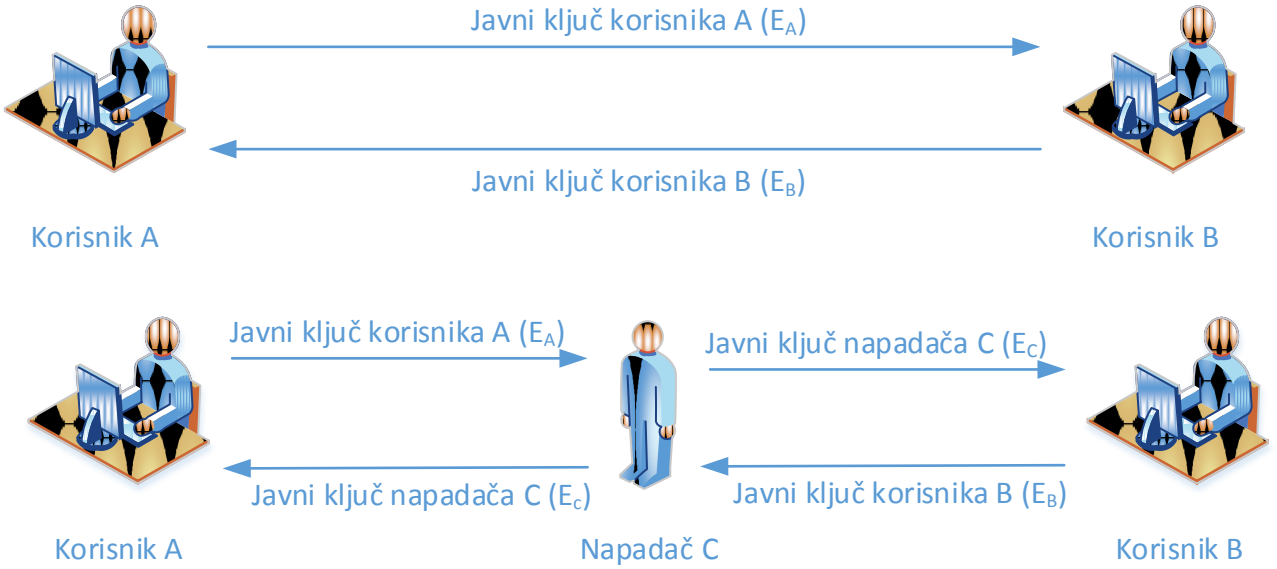
- Digitalni potpis jamči autentičnost i cjelovitost primljene poruke
  - Ali postaje problem kada treba potpisivati velik broj poruka
- U takvim situacijama upotrebljavamo sljedeći sustav
  - Primatelj i pošiljatelj se dogovore o dijeljenoj tajni, slučajnom broju određene veličine (barem 128 bita), nazivo taj broj S
  - Za poruku koju treba slati pošiljatelj izračunava MD(P|S)
    - Okomita crta označava konkatenaciju bitova!
  - Primatelj prima poruku M' i MD(P|S), izračunava MD(P'|S) i uspoređuje s primljenim sažetkom. Ako su isti, onda je primatelj siguran da je poruka autentična i nije mijenjana
  - Ovaj sustav se zove MAC (*message authentication code*) ili MIC (*message integrity code*)

Osiguranje tajnosti poruka

- Želimo li, uz autentičnost i cjelovitost, osigurati i tajnost tada poruku šifriramo
- Šifriranje ne može ići bez osiguranja autentičnosti i cjelovitosti
  - Obrnuto može
- Šifriranje se obavlja upotrebom simetrične kriptografije
- Pravilo je da se za šifriranje i osiguranje autentičnosti koriste različiti ključevi
  - I ključevi se periodički mijenjaju!
- Također je pravilo da se prvo radi zaštita šifriranje, a tek potom se dodaje kod za zaštitu integriteta i autentičnosti

Problem distribucije javnih ključeva

- Ipak ostaje i dalje problem razmjene ključeva
  - Kada primio nečiji javni ključ kako znamo da nam netko nije podmetnuo svoj javni ključ? Drugim riječima, kako znamo da nije u tijeku MITM napad ili lažno predstavljanje?



- Navedeni problem možemo pokušati riješiti na dva načina

Raspodijeljeni način distribucije javnih ključeva

- Ideja je da prilikom primanja javnog ključa koristimo nekakav alternativni način provjere ispravnosti
  - Nalazimo se na istom mjestu licem u lice pa odmah razmjenimo ključeve, telefonom tražimo osobu da nam izdiktira sažetak ključa, negdje na Internetu provjerimo ključ
  - U krajnjem slučaju jednostavno vjerujemo da je to to (leap of faith)
  - Od tada na dalje očekujemo uvijek isti ključ i ako dobijemo nešto različito tada smatramo da se netko pokušava ubaciti u komunikaciju.
  - Ovaj pristup koriste PGP (engl. Pretty Good Privacy), SSH
  - Problem je što rješenje ne skalira, **nema centralnog nadzora**

Infrastruktura javnog ključa – Ideja

- Postoji organizacija kojoj **svi vjeruju**
  - **certifikacijsko tijelo** (engl. certificate authority, CA)
  - Ima svoj javni i tajni ključ. **Javni ključ imaju SVI na Internetu**
- Certifikacijsko tijelo izdaje **certifikate** korisnicima
  - Certifikat (engl. certificate) je podatkovna struktura koja sadrži podatke o korisniku (ime, adresa, Web, mail, …), vrijeme važenja certifikata, **javni ključ korisnika** i eventualno druge podatke.
  - Certifikat je **potpisan** od strane certifikacijskog tijela!
    - Svi koji imaju javni ključ certifikacijskog tijela mogu provjeriti potpis i biti sigurni da je certifikat ispravan te da pripada navedenom korisniku!
    - Prije potpisivanja CA provjerava korisnika (telefonski ili na neki drugi način)
- Certifikacijsko tijelo izdaje certifikat samome sebi!
  - To se zove samopotpisani certifikat (engl. self signed certificate)

Infrastruktura javnog ključa – Implementacija (1)

- Postoji više certifikacijskih tijela
- Certifikacijska tijela delegiraju provjeru korisnika registracijskim tijelima (engl. registration authority)
- „Korisnik” kome se izdaje certifikat može biti osoba, ali i Web stranica, poslužitelj, …
- Distribucija certifikata certifikacijskih tijela obavlja se sa aplikacijama koje koriste certifikate, odnosno PKI
  - Primjerice, svi Web preglednici dolaze s popisom certifikacijskih tijela kojima vjeruju
- U praksi CA-ovi rade propuste jer su u pitanju komercijalne tvrtke koje zarađuju na izdavanju certifikata
  - Primjeri tvrtki: VeriSign

Infrastruktura javnog ključa – Implementacija (2)

- Tehnički svatko može osnovati svoje certifikacijsko tijelo
  - ALI, jako je teško biti priznat i uključiti certifikat u Web preglednike
- Izdavanje certifikata se uglavnom naplaćuje
  - Pogotovo za Web poslužitelje
- Zbog naplaćivanja često se koriste samopotpisani certifikati (engl. selfsigned certificates)
  - Korisnik generira javni i tajni ključ, slaže certifikat (popunjava podatkovnu strukturu) i potpisuje svojim tajnim ključem!
  - Web preglednici kada dobiju takve certifikate upozoravaju korisnika da se stranici ne može vjerovati, a na korisniku je da odluči što dalje

Završne napomene u vezi kriptografije

- Prošli smo samo vrlo mali dio kriptografije i primjene
- Kriptografija je složena i razvoj novih algoritama i protokola je izuzetno složen
  - Razvoj AES-a pet godina, algoritma za izračuvanavanje sažetaka također pet godina. Razvoj obavljaju timovi!
- Uprkos stručnosti i broju osoba koje razvijaju protokole i algoritme, dešavaju se propusti
- Međutim, ni implementacija nije jednostavna, loša implementacija omogućava otkrivanje ključeva i niz drugih stvari
- Zaključak: **ne izmišljati svoje, ne implementirati svoje, koristiti postojeće i provjereno!**

Sigurnost komunikacije na Internetu

Protokoli IPsec i SSL/TLS

Arhitektura IPsec (1)

- Arhitektura definira dva protokola čija zadaća je prijenos podataka koji se štite tijekom prijenosa
  - Protokol AH: zaglavlje autentičnosti (engl. *Authentication Header*, AH): štiti integritet datagrama, autentičnost izvora, neponavljanje
  - Protokol ESP: sigurnosno ovijeni podaci (engl. *Encapsulating Security Payload*, ESP): tajnost i integritet datagrama, autentičnost izvora, neponavljanje
  - Za oba protokola je definiran transportni i tunelski način rada
  - Protokoli ESP i AH se nalaze u mrežnom sloju te mogu štiti bilo koji protokol koji se prenosi korištenjem protokola IP
    - To je razliku u odnosu na protokol TLS o kojemu pričamo malo kasnije

Arhitektura IPsec (2)

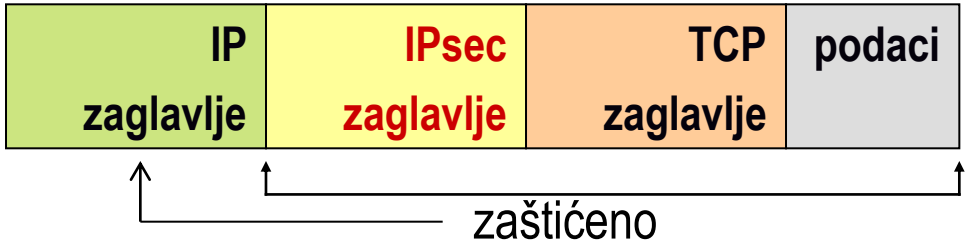
- Dodatno, definiran je protokol IKE (*Internet Key Exchange*) čija zadaća je autentifikacija čvorova, dogovaranje kriptografskih algoritama koji će se koristiti za zaštitu, ključeva, te povremenu promjenu ključeva.
- IETF je definirao tri verzije arhitekture IPsec. Trenutno se najviše koristi verzija 2, dok se najnovija verzija 3 (iz 2010. godine) polako uvodi u širu upotrebu.
- U verziji tri koristi se IKEv2 te je protokol AH definiran kao opcionalan a ESP se mora implementirati

Sigurna komunikacija uz IPsec

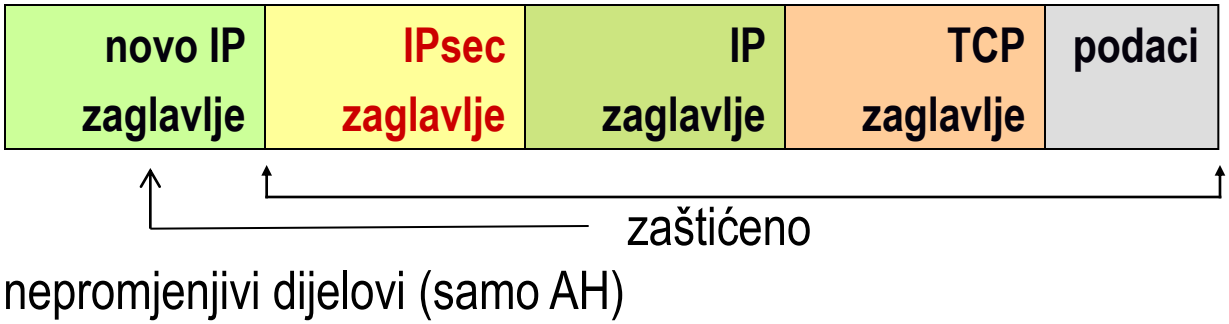
izvorni IP-datagram

Transportni način: štiti podatke protokola viših slojeva (od transportnog na više)

datagram zaštićen transportnim načinom



Tunelski način: štiti cijeli izvorni IP-paket



datagram zaštićen tunelskim načinom

Primjena arhitekture IPsec

- Vrlo široka primjena za ostvarivanje virtualnih privatnih mreža (engl. Virtual Private Networks, VPN)
  - Za ovo se koristi ESP u tunelskom način rada. Na taj način krajnje točke komunikacije ne znaju za tuneliranje a kada je paket na Internetu potencijalni napadači ne mogu saznati ništa o unutarnjoj mreži (primjerice IP adrese)
- Moguće je ostvariti i sigurnu komunikaciju dva direktno spojena računala, primjerice poslužitelja i klijenta
  - Može se upotrebljavati za neke kritičnije situacije
- Problem arhitekture IPsec je u njenoj složenosti i transparentnosti (!)

Protokol za sigurnost transportnog sloja (1)

TLS (engl. *Transport Layer Security*)

- Protokol koji se razvija unutar IETF, zadnja verzija 1.2
- Zadaće protokola TLS
  - Omogućiti klijentu utvrđivanje identiteta poslužitelja (autentikacija), protokol podržava i autentikaciju klijenta poslužitelju ali se to rijetko koristi.
  - Zaštita komunikacija od prisluškivanja, lažiranja, ponavljanja, izmjene, fabrikacije
- Koristi protokol TCP za prijenos podataka

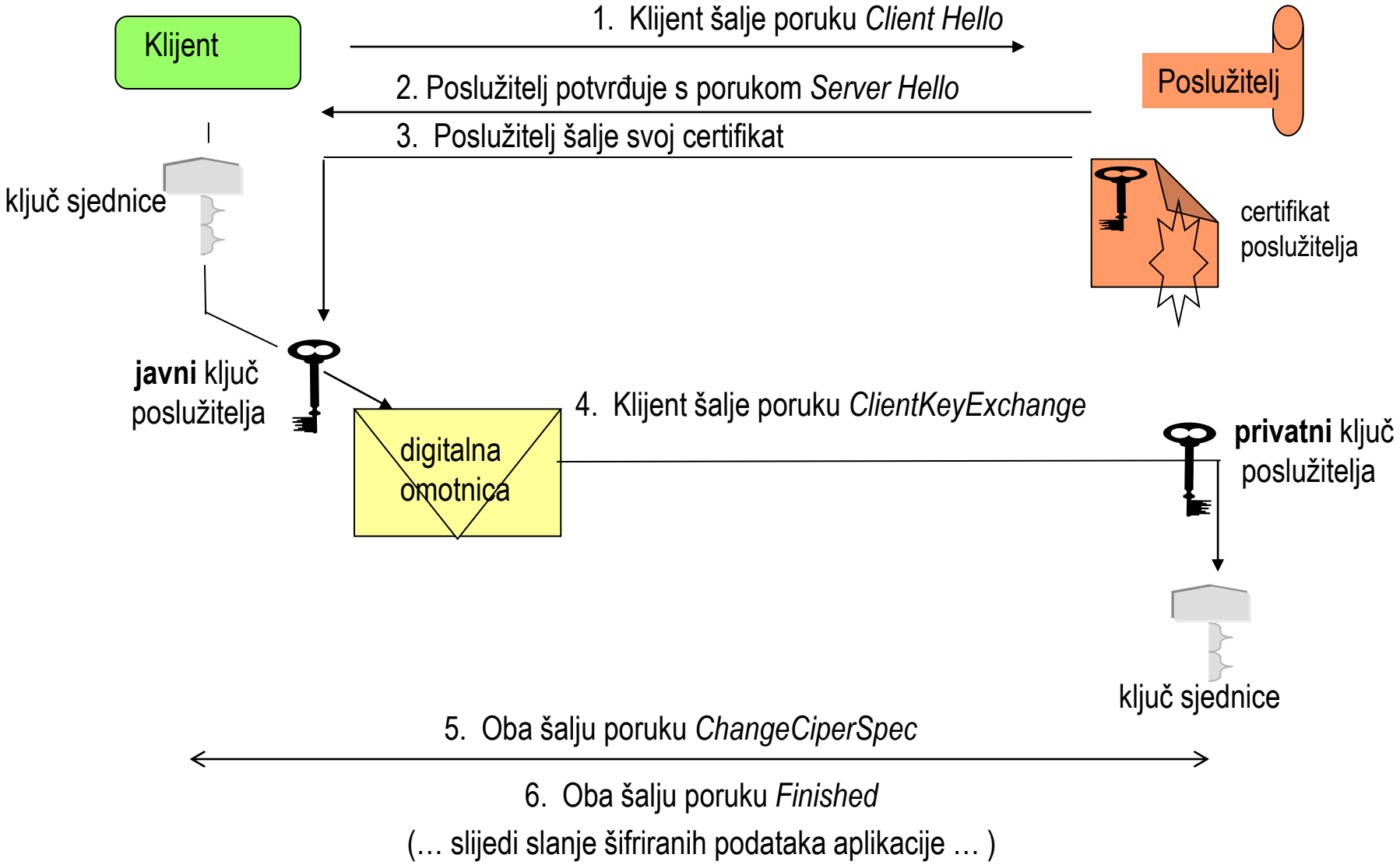
SSL (engl. *Secure Sockets Layer*)

- Originalna inačica koju je osmislio Netscape ali koja se više **ne smije koristiti** zbog propusta u sigurnosti!

Protokol za sigurnost transportnog sloja (2)

- Za autentifikaciju se koriste certifikati!
- Usluge tog protokola dizajnirane su na takav način da ga aplikacije mogu koristiti s minimalnim izmjenama
  - Umjesto direktnog poziva funkcija za slanje i primanje podatka, zovu se funkcije koje će prvo obaviti šifriranje i zaštitu integriteta a potom poslati podatke na drugu stranu.
  - U praksi promjena ipak nije tako jednostavna jer kriptografija i kriptografski protokoli nisu jednostavni!
- U nastavku ćemo detaljnije pogledati samo uspostavu TLS sjednice tijekom koje se
  - Poslužitelj autentificira klijentu, te se
  - Razmjenjuju sjednički ključevi (za šifriranje i zaštitu integriteta!)

Uspostavljanje TLS-sjednice

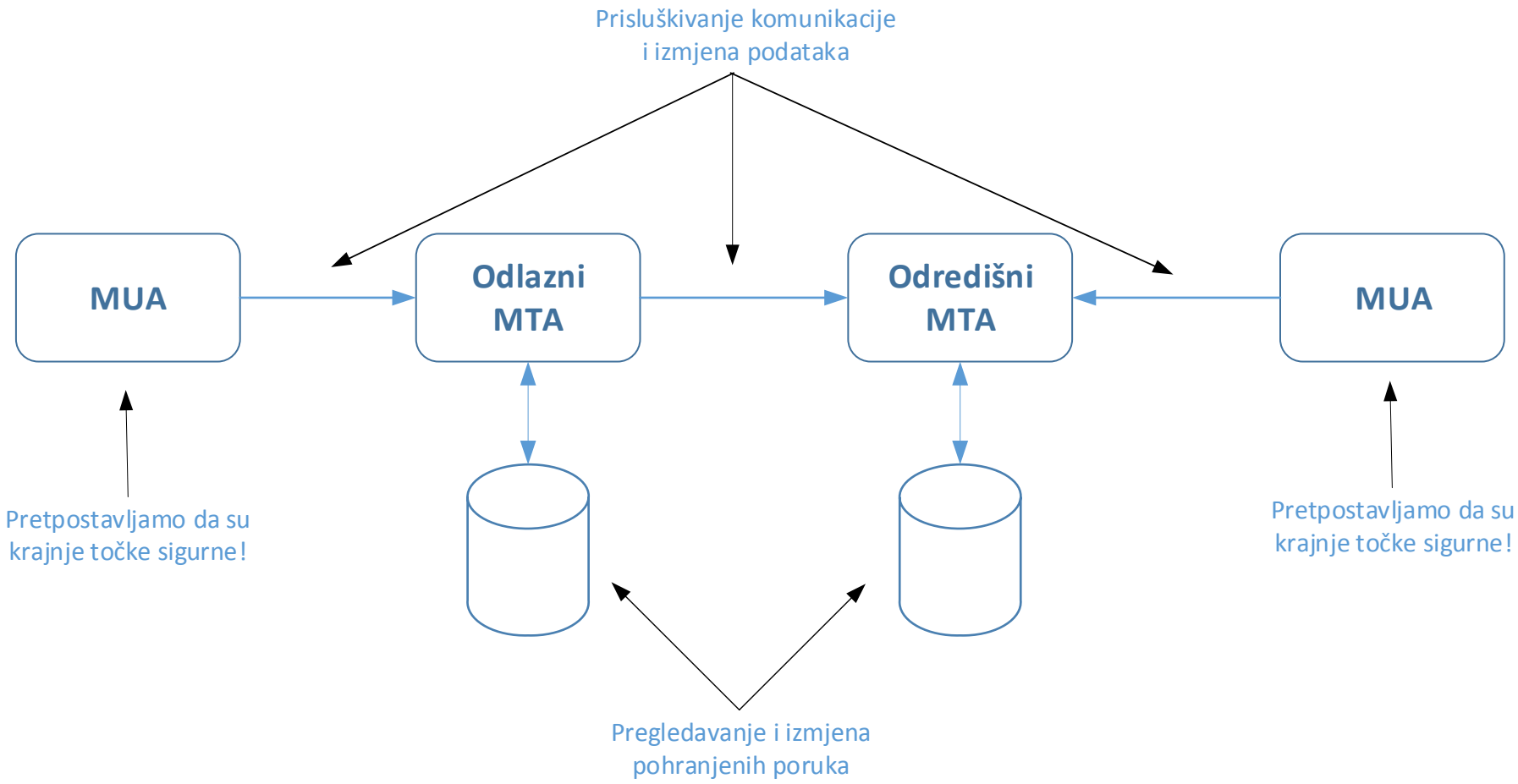


Poboljšanje sigurnosti Weba

- Problemi protokola HTTP preko TCP-a su
  - Nismo sigurni je li poslužitelj kojemu pristupamo onaj za kojeg se on predstavlja.
  - Svatko može pratiti komunikaciju koja sadrži osjetljive podatke (lozinke i slično).
  - Bilo tko tko se nalazi na komunikacijskom putu može mijenjati komunikaciju i ubacivati lažne informacije
- To su vrlo ozbiljni problemi zbog kojih se komunikacija radi zaštite odvije preko protokola TLS
  - To je naznačeno sa prefiksom https u URL-u, a podrazumijevani port u tom slučaju je 443
  - Ovo ne znači da više ne treba brinuti jer napadači mogu neoprezne korisnike prevariti bez obzira na korištenje protokola https!

Problemi sigurnosti elektroničke pošte

- Problemi elektroničke pošte



Sigurnost komunikacije elektroničke pošte

- Ako pretpostavimo da su svi poslužitelji sigurni, tada je dovoljno zaštiti komunikaciju
- Moramo štiti komunikaciju zbog
  - Prijenosa lozinki, mogućnosti da netko snima promet, neovlaštena izmjena poruka tijekom prijenosa
- Zaštita komunikacije se može obaviti tako da se SMTP/POP/IMAP prenose preko protokola TLS
  - To se koristi na dva načina, odmah se kreće sa TLS protokolom za što je rezerviran poseban port (IMAPS na portu 993), ili se krene s „običnim” protokolom pa se prebacina TLS (STARTTLS naredbe u protokolu).
- Problem je što ne možemo jamčiti da će SVA komunikacija ići preko protokola TLS

Sigurnost poruka elektroničke pošte

- Najbolje rješenje je potpisivanje i/ili kriptiranje poruka elektroničke pošte
  - Na taj način se može jamči autentičnost i cjelovitost te po potrebi i tajnost!
- Koriste se dvije norme S/MIME te PGP
- Problem je što klijenti elektroničke pošte variraju u podršci navedenih normi

Sigurnost poruka elektroničke pošte – S/MIME

- S/MIME se temelji na sustavu PKI
  - engl. Secure MIME
- Svaki korisnik ima svoj privatni ključ i certifikat.
  - Korisnik može sam generirati svoj privatni i javni ključ te zatražiti izdavanje certifikata.
  - U korporativnim okruženjima korisnik dobija svoj privatni ključ i certifikat od odgovarajuće službe u tvrtci
- Ovo je dobro rješenje za korporativna okruženja
  - Specifično namijenjeno zaštiti elektroničke pošte

Sigurnost poruka elektroničke pošte – PGP

- PGP se temelji na međusobnom dijeljenju javnih ključeva bez centraliziranog nadzora.
  - Skraćenica od *Pretty Good Privacy*
  - Prvu verziju razvio i napisao Phil Zimmermann 1991. godine
  - Često se pod tim porazumijeva i program za šifriranje, potpisivanje, itd.
- Normirano u sklopu RFC4880 (OpenPGP)
- Pogodniji je za pojedince i slabo povezane grupe
- Može se koristiti za šifriranje i potpisivanje bilo kakvih podataka
  - Nije specifično za poruke elektroničke pošte

Uređaj za zaštitu mreža i sustava: Vatrozid

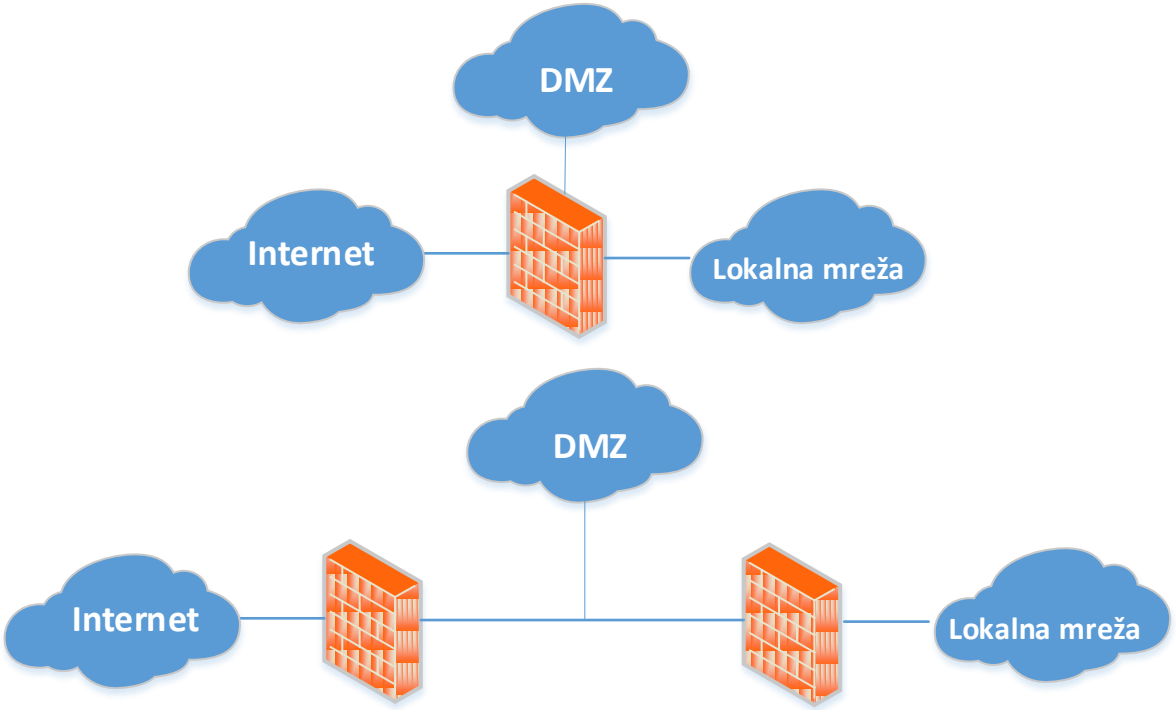
- Uređaj koji radi na mrežnom sloju i nadzire promet koji kroz njega prolazi
  - Njegova zadaća je **sigurnost krajnjih sustava i mreža, a ne komunikacije**!
- Sadrži bazu pravila i svaki paket koji dođe se provjerava s tom bazom
  - Svako pravilo definira karakteristike paketa na kojeg se odnosi (primjerice, izvorišne ili odredišne adrese, protokoli, portovi, …)
  - Drugu dio pravila definira akciju koju je potrebno poduzeti ako paket odgovara pravilu. Osnovne akcije su: ODBACI ili PROPUSTI
  - Dobra praksa kod podešavanja vatrozida je da se ne dopušta ništa što nije eksplicitno dozvoljeno!

Vrste vatrozida

- Bez stanja (engl. stateless)
  - Za svaki ispitani paket koji prolazi ne čuva se nikakvo stanje, svi paketi su međusobno nezavisni.
  - To može stvoriti probleme kod protokola koji očekuju otvorena oba smjera kao što je TCP
    - Moramo omogućiti da sa Interneta dolaze SYN+ACK paketi, ali s obzirom da ne znamo koji port će izabrati računalo u unutarnjoj mreži moramo otvoriti raspon portova!
  - Brži, ali teži za podešavanje i nesigurniji
- Sa stanjem (engl. statefull)
  - Kod podešavanja čuvaju informaciju o viđenim paketima
    - To znači da mogu automatski otvoriti drugi smjer komunikacije kada treba!
  - Sporiji, ali jednostavniji za podešavanje i sigurniji

Arhitekture mreža s vatrozidom

- Ako u mreži koja se štiti postoje poslužitelji kojima treba pristupiti izvana, tada se oni smještaju u posebnu mrežu
  - Demilitarizirana zona (DMZ)
- Upotrebljavaju se arhitekture s jednim ili dva vatrozida



Završne napomene o vatrozidu

- Vatrozid je uređaj mrežnog sloja. No, s obzirom da su mu mogućnosti u tom slučaju ograničene svoju funkcionalnost obavlja i na prijenosnom sloju.
- Na aplikacijskom sloju se često koriste aplikacijski posrednici koji „razumiju” pojedini protokol i mogu detaljnije filtrirati promet
  - Primjerice česti su aplikacijski posrednici za SMTP, HTTP
- Prilikom kupovine često je sva funkcionalnost upakirana u jedan uređaj koji proizvođači nazivaju samo vatrozid
- Vatrozid nije rješenje svih problema sigurnosti(!)
  - Sve više aplikacija koristi HTTP za komunikaciju kako bi zaobišli vatrozide.

Pitanja za provjeru znanja

- Kako se može utvrditi autentičnost (vjerodostojnost) sudionika u komunikaciji?
- Kako se može očuvati cjelovitost (integritet) poruke?
- Kako se može postići povjerljivost (tajnost) poruke?
- Koje sigurnosne zahtjeve ne rješavaju kriptografski postupci?
- Kakve se sigurnosne usluge pruža i što se štiti zaglavljem AH u tunelskom načinu rada?
- Kakve se sigurnosne usluge pruža i što se štiti zaglavljem ESP u transportnom načinu rada?

Istraživački zadatak

Istražite pretraživanjem informacija dostupnih putem Interneta:

- Što obuhvaća pojam "*Authentication Authorisation Accounting*" (AAA) u Internetu?
- Kako su AAA usluge izvedene u CARnetu?
- Kad su Vam te usluge potrebne?

Dodatna literatura

- A. Bažant, Ž. Car, G. Gledec, D. Jevtić, G. Ježić, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, Z. Skočir:

  "Telekomunikacije – tehnologija i tržište", 6. Sigurnost i privatnost, Element, Zagreb, 2007.
- L. Budin, M. Golub, D. Jakobović, L. Jelenković:

  "Operacijski sustavi", 11. Sigurnost računalnih sustava,

  Element, Zagreb, 2010.

- The Handbook of Applied Cryptography Online
  http://www.cacr.math.uwaterloo.ca/hac/
- An Overview of Cryptography
  http://www.garykessler.net/library/crypto.html