
Sigurnost računalnih mreža

Poglavlje 10 — Skripta kolegija *Računalne mreže*

doc. dr. sc. Sandi Baressi Šegota

Fakultet informatike Sveučilišta Jurja Dobrile u Puli

Poglavlje 10

Sigurnost računalnih mreža

Mrežna sigurnost bavi se zaštitom komunikacije u prisutnosti napadača. Četiri su temeljna cilja: **povjerljivost** (samo ovlašteni čitaju poruku), **integritet** (poruka nije neopaženo izmijenjena), **autentikacija** (strane su onaj tko tvrde da jesu) i **dostupnost** (usluga radi). U ovom poglavlju obrađujemo kriptografiju (simetričnu i asimetričnu), mehanizme integriteta i autentikacije (hash, MAC, digitalni potpis, certifikati) te sigurne protokole i uređaje (TLS, IPsec, vatrozidi).

Ishodi učenja

Po završetku poglavlja student će moći: navesti ciljeve sigurnosti; razlikovati simetričnu i asimetričnu kriptografiju; objasniti hash, MAC i digitalni potpis; opisati certifikate i PKI; te objasniti TLS, IPsec i vatrozide.

Pretpostavljamo aktivnog napadača („Trudy”) koji može prisluškivati promet, mijenjati i ubacivati pakete te se lažno predstavljati. Vrijedi i **Kerckhoffsovo načelo**: sustav mora biti siguran čak i kad je algoritam poznat — tajnost počiva isključivo na *ključu*, pa se koriste javni, dobro proučeni algoritmi.

10.1 Kriptografija

Kod **simetrične** kriptografije obje strane dijele *isti* tajni ključ kojim se poruka i šifrira i dešifrira. Takve su šifre (npr. AES) vrlo brze, ali nameću problem: kako sigurno *razmijeniti* zajednički ključ preko nesigurnog kanala. Otpornost na napad grubom silom raste s duljinom ključa — svaki dodatni bit udvostručuje prostor ključeva, pa su AES-128/256 praktički neprobojni iscrpnim pretraživanjem.

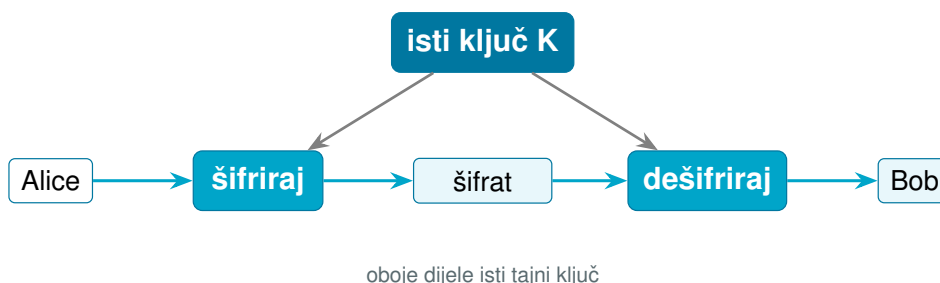


Figure 10.1: Simetrična kriptografija: isti tajni ključ za šifriranje i dešifriranje.

Kod **asimetrične** (kriptografije javnog ključa) svaka strana ima *par* ključeva: *javni* (koji se slobodno dijeli) i *privatni* (tajan). Poruka šifrirana javnim ključem može se dešifrirati samo

pripadnim privatnim ključem. Time se rješava razmjena ključa, no asimetrične su operacije spore, pa se u praksi koristi *hibridni* pristup: asimetrično se dogovori (ili razmjenom tipa **Diffie-Hellman** izvede) *sesijski* simetrični ključ, a podaci se potom šifriraju brzom simetričnom šifrom. Tako radi i TLS.

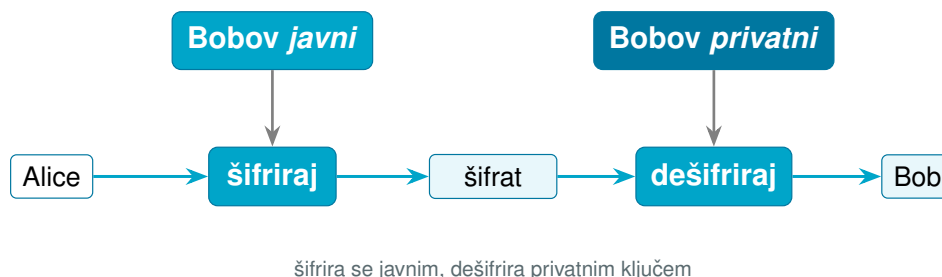


Figure 10.2: Asimetrična kriptografija: šifriranje javnim, dešifriranje privatnim ključem.

	simetrična	asimetrična
ključevi	jedan zajednički	par (javni/privatni)
brzina	vrlo brza	spora
razmjena ključa	problematična	riješena
uporaba	masovni podaci	ključevi, potpisi

Table 10.1: Usporedba simetrične i asimetrične kriptografije.

10.2 Integritet, potpis i autentikacija

Hash funkcija poruci pridružuje kratki „otisak“; i najmanja promjena poruke daje posve drukčiji otisak, pa se otisak koristi za provjeru *integriteta*. Dobra hash funkcija (npr. SHA-256) je *jednosmjerna* i *otporna na sudare*. Ako se u izračun uključi tajni ključ, dobiva se **MAC** (*message authentication code*), koji uz integritet jamči i *autentičnost* pošiljatelja.

Digitalni potpis koristi asimetričnu kriptografiju obrnuto: pošiljatelj potpisuje otisak poruke svojim *privatnim* ključem, a bilo tko provjerava potpis *javnim* ključem. Time se osim integriteta postiže i *neporecivost* (pošiljatelj ne može zaniijekati da je potpisao).

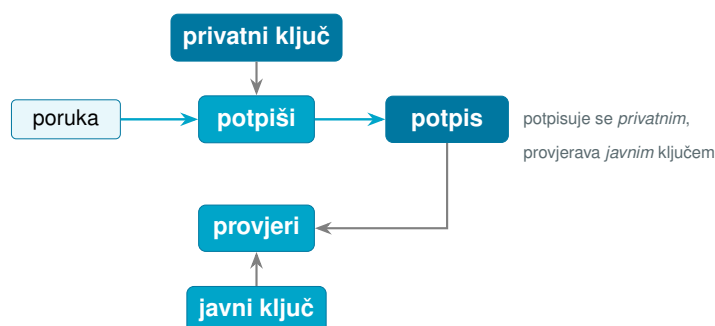


Figure 10.3: Digitalni potpis: potpisivanje privatnim, provjera javnim ključem.

Preostaje pitanje: kako znati da neki javni ključ *doista* pripada određenoj strani? Odgovor je **certifikat** — javni ključ zajedno s identitetom, digitalno potpisan od strane pouzdanog

certifikacijskog tijela (CA). Skup CA-ova, certifikata i pravila opoziva čini **PKI** (infrastrukturu javnog ključa); preglednici dolaze s popisom povjerljivih korijenskih CA-ova i provjeravaju lanac povjerenja. Za autentikaciju se koristi i *nonce* (jednokratni broj) koji sprječava **napad ponavljanjem** (replay), gdje napadač snima valjanu poruku i kasnije je ponovno šalje.



Figure 10.4: Certifikat: CA potpisom jamči da javni ključ pripada određenom subjektu.

10.3 Sigurni protokoli i uređaji

TLS osigurava transportni sloj i pretvara HTTP u **HTTPS**. Pri rukovanju poslužitelj šalje certifikat, strane dogovaraju sesijski ključ, a nakon toga sva aplikacijska komunikacija teče šifrirano; TLS tako jamči autentikaciju poslužitelja te povjerljivost i integritet podataka. **IPsec** štiti promet na mrežnom sloju i temelj je **VPN**-a: uspostavlja šifrirani tunel između mreža ili uređaja preko nepovjerljive mreže.

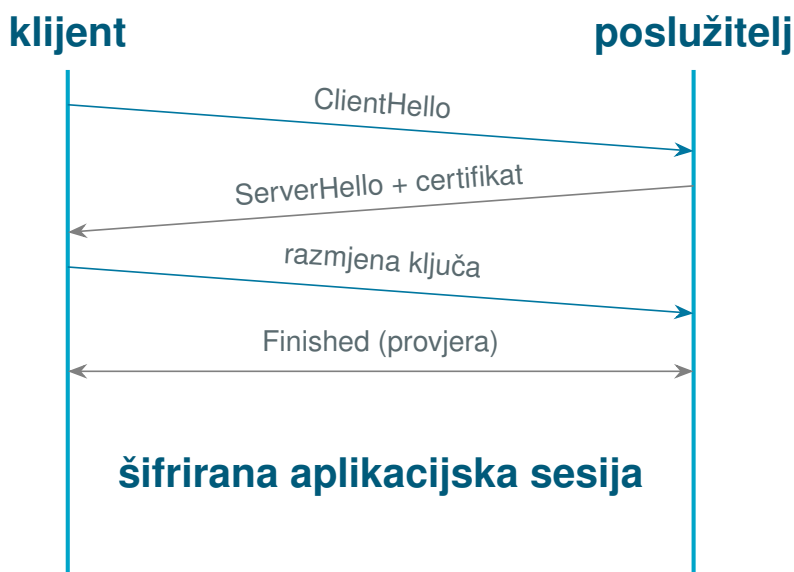


Figure 10.5: TLS rukovanje: certifikat i dogovor ključa, potom šifrirana sesija.

Vatrozid filtrira promet između unutarnje mreže i Interneta prema *pravilima* (po adresi, portu, stanju veze). Razlikujemo filtriranje paketa (bez konteksta), *stateful* vatrozide (prate stanje veza) i aplikacijske gatewaye (proxy koji gleda sadržaj). Uz njih se koriste sustavi za *otkrivanje* (**IDS**) i *sprječavanje* (**IPS**) upada, koji prepoznaju poznate napade i anomalije. U praksi se primjenjuje *dubinska obrana* — više slojeva zaštite i načelo najmanje privilegije — jer nijedan pojedinačni mehanizam nije savršen, a najslabija je karika često sam korisnik (phishing).

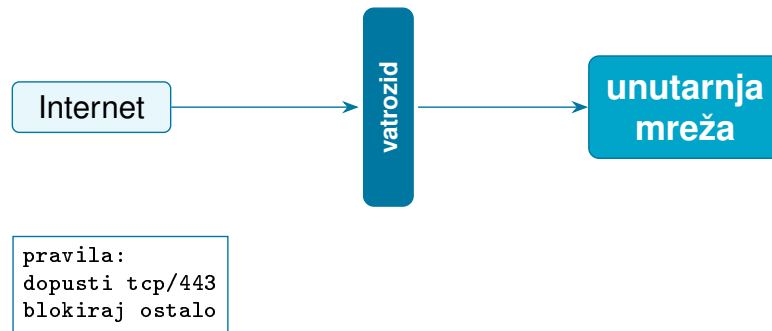


Figure 10.6: Vatrozid propušta ili blokira promet prema definiranim pravilima.

Sažetak poglavlja

Ciljevi sigurnosti su povjerljivost, integritet, autentikacija i dostupnost. *Simetrična* kriptografija je brza, a *asimetrična* rješava razmjenu ključa (u praksi hibridno). **Hash** i **MAC** štite integritet, a **digitalni potpis** dodaje neporecivost; **certifikati** i **PKI** vežu javni ključ za identitet. **TLS** štiti transport (HTTPS), **IPsec** mrežni sloj (VPN), a **vatrozidi** i **IDS/IPS** kontroliraju promet uz dubinsku obranu.