

Sigurnost računalnih mreža

Predavanje 10 • kolegij Računalne mreže

doc. dr. sc. Sandi Baressi Šegota

Fakultet informatike Sveučilišta Jurja Dobrile u Puli

Sadržaj predavanja

- 1 Osnove sigurnosti
- 2 Kriptografija
- 3 Integritet i autentikacija
- 4 Sigurni protokoli
- 5 Sažetak

Osnove sigurnosti

Ishodi učenja

Nakon ovog predavanja moći ćete:

- navesti **ciljeve** mrežne sigurnosti;
- razlikovati **simetričnu** i **asimetričnu** kriptografiju;
- objasniti **integritet** (hash, MAC) i **digitalni potpis**;
- opisati **certifikate** i PKI;
- objasniti **TLS**, **IPsec** i **vatrozide**.

Ciljevi sigurnosti

povjerljivost

integritet

dostupnost

autentikacija

četiri temeljna cilja sigurnosti

- **povjerljivost**: samo ovlašteni čitaju
- **integritet**: poruka nije izmijenjena
- **dostupnost** i **autentikacija**

Prijetnje i napadači

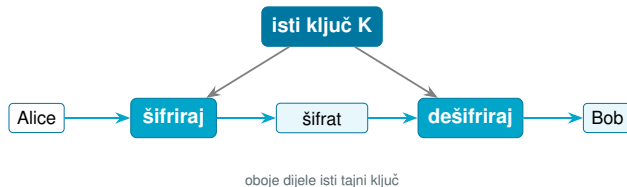
- „Trudy” može **prisluškivati**, **mijenjati**, **lažirati**
- **presretanje** (sniffing), **ubacivanje**, **uskraćivanje** (DoS)
- pretpostavljamo da napadač **vidi** mrežu

Što napadač može učiniti?

- **prisluškivati** promet (povjerljivost)
- **izmijeniti** ili ubaciti pakete (integritet)
- **lažno se predstaviti** (autentikacija)
- **preopteretiti** uslugu (dostupnost)

Kriptografija

Simetrična kriptografija



- isti **tajni** ključ za šifriranje i dešifriranje
- brza (npr. **AES**), ali treba *sigurno* razmijeniti ključ

Problem razmjene ključa

- kako dvije strane dobiju **zajednički** tajni ključ?
- preko nesigurnog kanala to je **teško**
- rješenje: **asimetrična** kriptografija

Kerckhoffsovo načelo

Sigurnost je u ključu

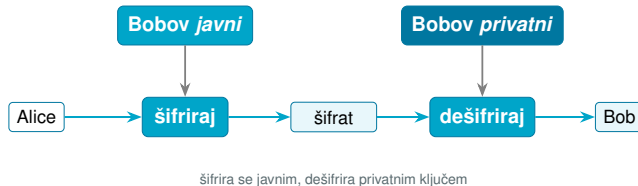
Sustav mora biti siguran čak i ako je **algoritam** poznat — tajnost počiva na **ključu**, ne na skrivanju metode.

Zato se koriste **javni**, dobro proučeni algoritmi.

Duljina ključa i napad grubom silom

- napad **grubom silom**: isprobati sve ključeve
- svaki dodatni bit **udvostručuje** prostor ključeva
- zato AES-128/256: praktički **neprobojni** silom

Asimetrična kriptografija



- par ključeva: **javni** (dijeli se) i **privatni** (tajan)
- šifrira se javnim, dešifrira **privatnim** ključem

RSA: ideja

- temelji se na težini **faktorizacije** velikih brojeva
- javni i privatni ključ matematički **povezani**
- spor za velike podatke $\Rightarrow$ koristi se za *ključeve*, ne za sve

Hibridni pristup

- asimetrično se dogovori **sesijski** simetrični ključ
- potom se podaci šifriraju **brzom** simetričnom šifrom
- najbolje od oba svijeta (tako radi TLS)

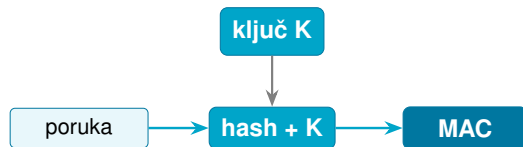
Diffie-Hellman razmjena ključa

- dvije strane **javno** razmijene vrijednosti
- svaka izračuna *isti* tajni ključ, ali ga napadač **ne** može
- omogućuje tajni ključ preko **javnog** kanala

Integritet i autentikacija

Hash i MAC

- **hash**: kratki „otisak” poruke
- promjena poruke $\Rightarrow$ drukčiji otisak
- **MAC**: hash s *ključem* (autentičnost)



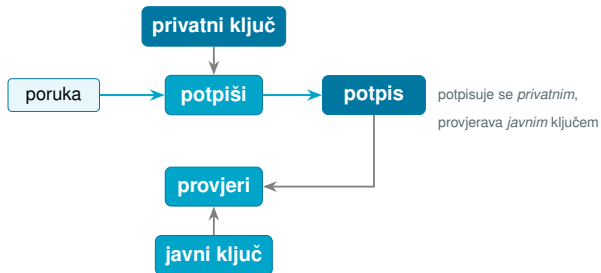
otisak štiti *integritet*; s ključem daje autentičnost (MAC)

Svojstva hash funkcija

- **jednosmjerne**: iz otiska se ne dobiva poruka
- **otporne na sudare**: teško naći dvije iste
- primjeri: **SHA-256** (izbjegavati stari MD5/SHA-1)

Digitalni potpis

- potpiši **privatnim** ključem
- provjeri **javnim** ključem
- daje integritet + **neporecivost**



Certifikati i CA

- kako znati čiji je **javni** ključ?
- **certifikacijsko tijelo** (CA) potvrđuje vezu
- **certifikat** = potpisani javni ključ



CA jamči: ovaj javni ključ pripada Bobu

PKI

- **infrastruktura javnog ključa**: CA, certifikati, opoziv
- preglednici imaju popis **povjerljivih** CA
- lanac povjerenja od korijenskog CA do poslužitelja

Autentikacija

- cilj: dokazati **tko si** (a ne samo tvrditi)
- **nonce** (jednokratni broj) sprječava *ponavljanje* (replay)
- kombinira se s potpisom/MAC-om

Napad ponavljanjem (replay)

- napadač **snimi** valjanu poruku i kasnije je *ponovi*
- obrana: **nonce**, vremenske oznake, redni brojevi
- svaka autentikacija mora biti **svježa**

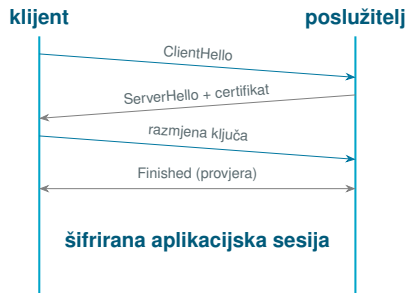
Sigurni protokoli

Sigurna e-pošta (PGP)

- **povjerljivost**: šifriraj sesijskim ključem
- **integritet + autentikacija**: potpiši otisak
- ključevi se razmjenjuju asimetrično

TLS: sigurni transport

- štiti HTTP $\Rightarrow$ **HTTPS**
- **rukovanje**: certifikat + dogovor ključa
- potom **šifrirana** sesija



TLS: što jamči

- **autentikacija** poslužitelja (certifikatom)
- **povjerljivost** i **integritet** podataka
- temelj sigurnog weba i mnogih aplikacija

IPsec i VPN

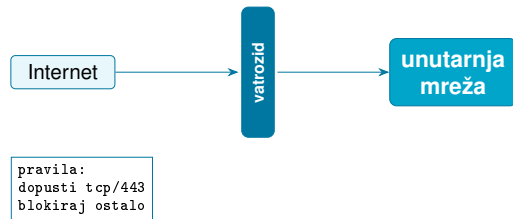
- štiti promet na **mrežnom** sloju
- **tunnel** između mreža/uređaja
- osnova **VPN**-a



IPsec štiti promet preko nepovjerljive mreže

Vatrozid (firewall)

- filtrira promet po **pravilima**
- razdvaja **unutarnju** mrežu od Interneta
- po adresi, portu, stanju veze



Vrste vatrozida

- **filtriranje paketa**: po adresi/portu (bez konteksta)
- **stateful**: prati *stanje* veza
- **aplikacijski gateway**: gleda sadržaj (proxy)

IDS/IPS

- **IDS**: otkriva sumnjiv promet i *upozorava*
- **IPS**: uz otkrivanje i *blokira*
- potpisi poznatih napada + **anomalije**

HTTPS u pregledniku

- **lokot** znači valjan certifikat i TLS sesija
- preglednik provjerava **lanac** do povjerljivog CA
- upozorenje na **nevaljan**/istekao certifikat

DDoS i dostupnost

- **distribuirani** napad preplavljuje uslugu prometom
- cilj: narušiti **dostupnost**
- obrana: filtriranje, **skaliranje**, mreže za ublažavanje

Dubinska obrana

- **više slojeva** zaštite (mreža, host, aplikacija)
- načelo **najmanje privilegije**
- nijedan mehanizam nije *savršen* $\Rightarrow$ kombiniraj ih

Ljudski faktor

- **phishing** i socijalni inženjering zaobilaze kriptografiju
- najslabija karika je često **korisnik**
- obrana: edukacija, **višefaktorska** autentikacija

Sažetak

Ključne poruke

- ciljevi: **povjerljivost, integritet, dostupnost, autentikacija**
- **simetrična** je brza, **asimetrična** rješava razmjenu ključa
- **hash/MAC** daju integritet, **potpis** i neporecivost
- **certifikati/PKI** vežu javni ključ za identitet
- **TLS, IPsec** i **vatrozidi** štite promet i mreže

Sljedeće predavanje

Računalstvo u oblaku I: IaaS/PaaS/SaaS, virtualizacija, kontejneri.

Pitanja za provjeru

- Koja su četiri cilja mrežne sigurnosti?
- Zašto se kombiniraju simetrična i asimetrična kriptografija?
- Koja je razlika između hasha i MAC-a?
- Čemu služi certifikat i tko ga izdaje?
- Što štiti TLS, a što IPsec?

Hvala na pažnji!

Pitanja i rasprava

doc. dr. sc. Sandi Baressi Šegota • FIPU