



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022/2023

Osnovni pojmovi



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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/>.

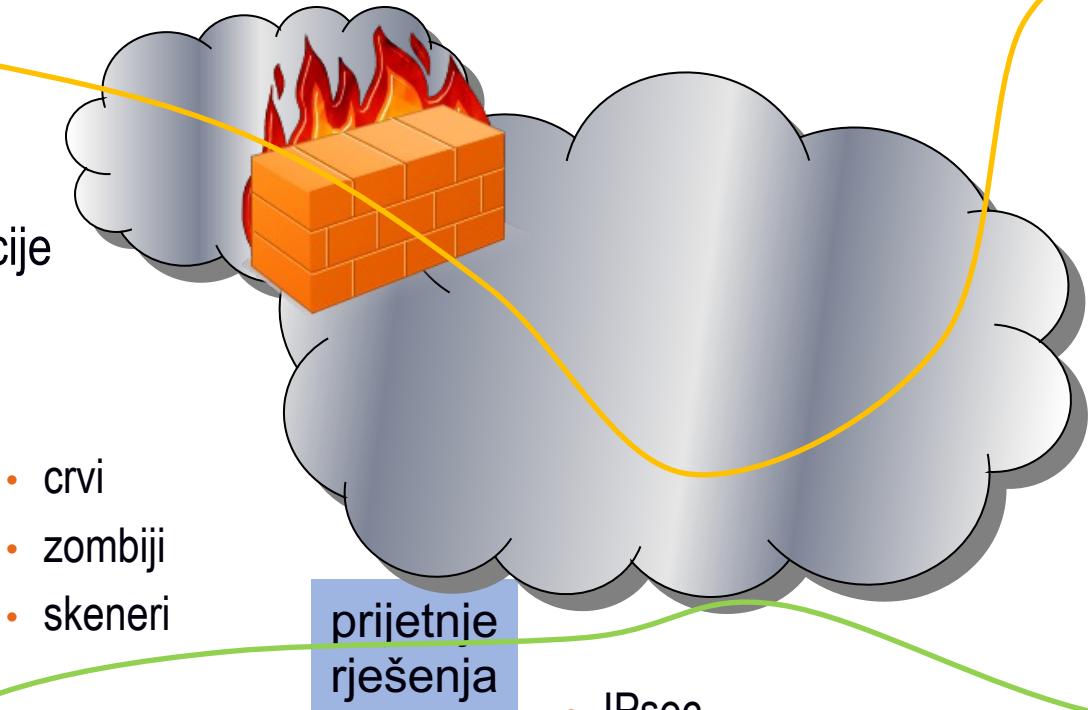
# Sigurnost mreža, usluga i aplikacija

sigurnost mreže



sigurnost aplikacije

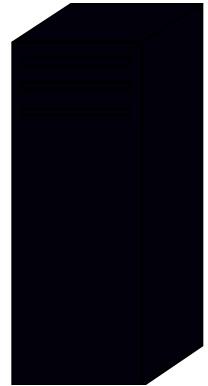
- virusi
- hoax
- malware
- spyware
- adware
- dialeri
- trojanci
- antivirus



prijetnje  
rješenja

- crvi
- zombiji
- skeneri
- firewall
- Intrusion Detection System

- IPsec
- demilitarizirana zona
- virtualne privatne mreže



sigurnost aplikacija  
i usluge

- cross site scripting
- ranjivosti
- Denial of Service
- lozinke
- lažna sjedišta
- kriptografija

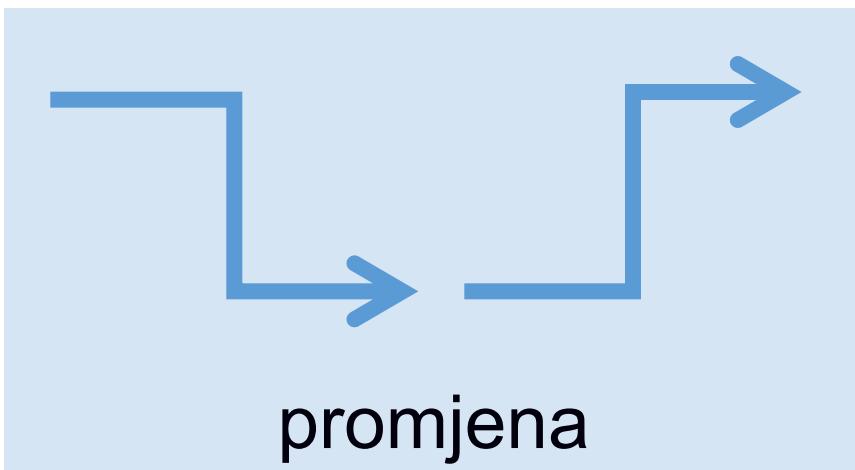
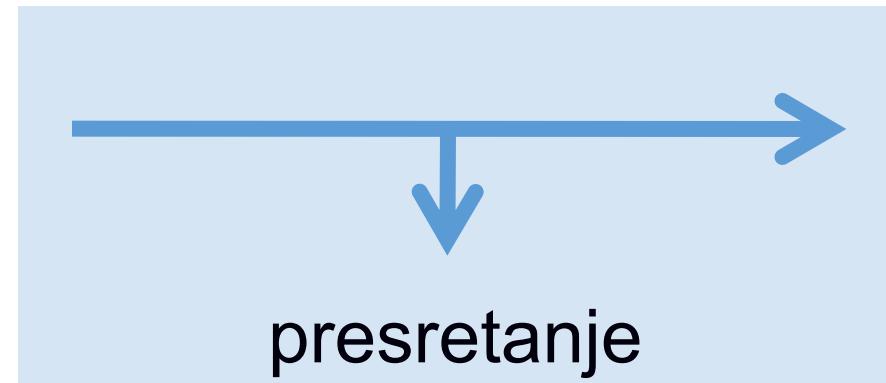
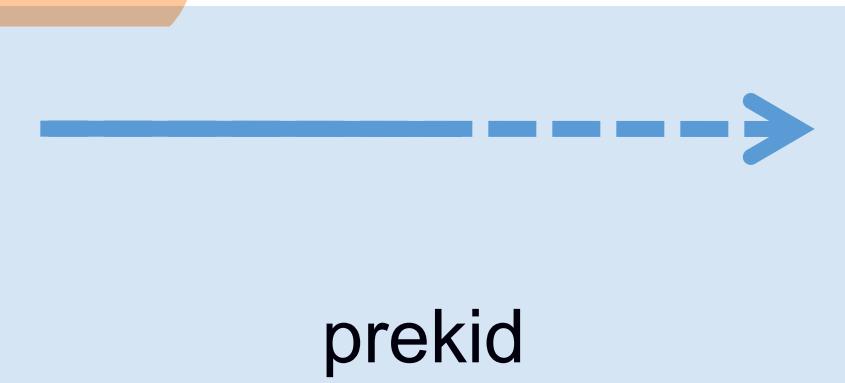
# Ranjivost, prijetnja, napad, nadzor

- mogući ciljevi: sklopolje, programska podrška, podaci
- **ranjivost:**
  - slabost u izvedbi sustava koju je moguće iskoristiti kako bi se izazvala šteta
  - *Zero-day ranjivost*
- **prijetnja:**
  - skup okolnosti koji može nanijeti štetu
- **napad:**
  - postupak u kojem se iskorištava ranjivost sustava
- **nadzor:**
  - mjere predostrožnosti
- prijetnja se sprječava nadzorom ranjivosti

# Pojam prijetnje

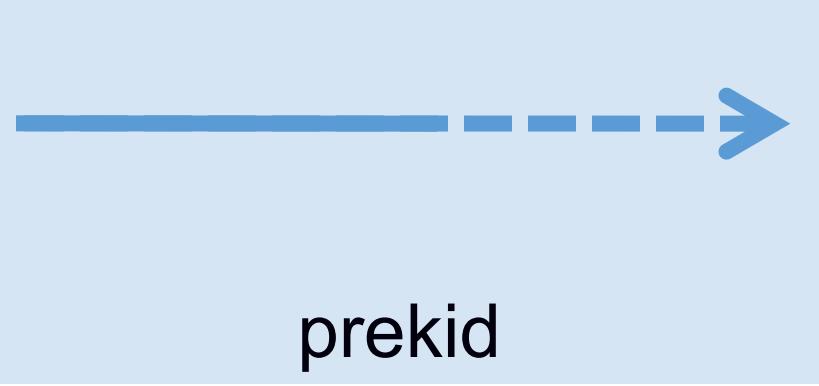
- prijetnja u mrežnom okruženju - okolnost, stanje ili događaj
  - cilj:
    - osoblje, mrežni ili računalni resursi
  - metode:
    - uništavanje, razotkrivanje ili modifikacija podataka
    - uskraćivanje usluge
    - prijevara
    - zlouporaba
  - vrste:
    - namjerna ili slučajna
    - aktivna ili pasivna
    - unutarnja ili vanjska

# Metode



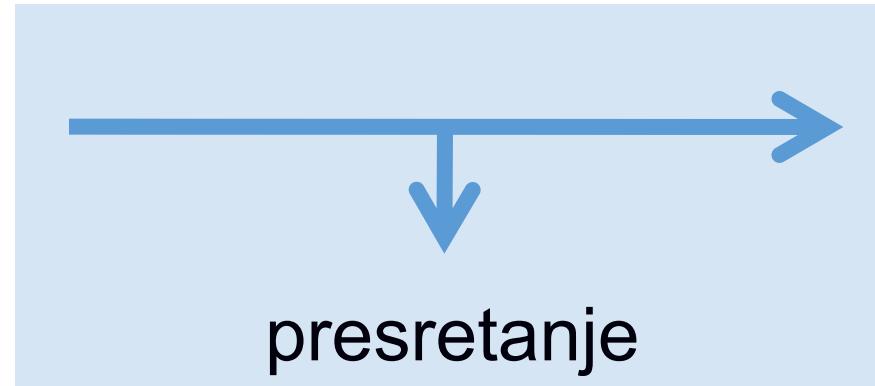
# Prekidanje komunikacije

- sustav nestaje, biva nedostupan ili neiskoristiv
  - uništavanje sklopolja
  - fizičko uništavanje komunikacijskih medija
  - ometanje komunikacije (šum)
  - narušavanje tablica usmjeravanja
  - brisanje programa ili datoteka
  - uskraćivanje usluge
  - Ukrajina 2022.!



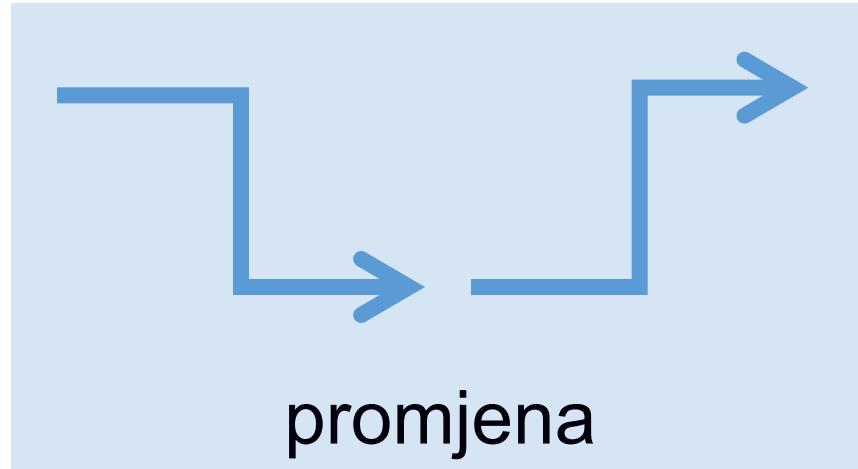
# Presretanje

- neovlaštena osoba ima pristup sustavu
  - prisluškivanje (*eavesdropping*)
  - nadzor mrežne komunikacije (*link monitoring*)
  - snimanje mrežnog prometa (*packet capturing*)
  - kompromitacija sustava (*system compromisation*)
- teško izbjegći kod bežične komunikacije i višeodredišnog i grupnog razašiljanja



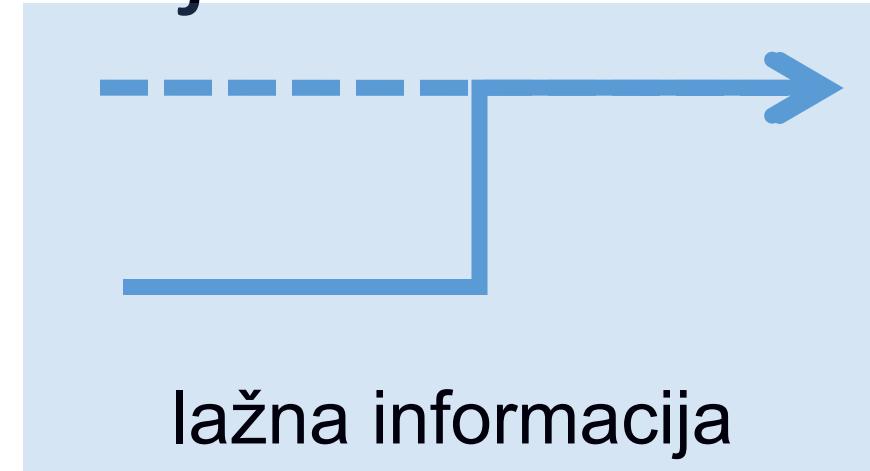
# Promjena podataka

- neovlaštena osoba mijenja sustav
  - mijenjanje zapisa u bazi podataka
  - kompromitiranje sustava
  - zlonamjerno iskorištavanje zastoja u komunikaciji
  - promjena sklopovske podrške



# Ubacivanje lažne informacije

- neovlaštena osoba stvara lažne informacije
  - dodavanje novih zapisu u bazu podataka
  - ubacivanje IP-datagrama u mrežu (*IP spoofing*)
  - lažne elektroničke poruke
  - lažna web-sjedišta



# Metode, prilike i motivi

- zlonamjerni napadač zadovoljava 3 uvjeta:
  - metoda:
    - vještina, znanje, alati i ostalo što mu omogućuje da izvede napad
  - prilika:
    - vrijeme i pristup sustavu
  - motiv:
    - razlog zbog kojeg želi napasti sustav
- često su mete sustavi koji imaju mnogo korisnika
  - Windows, IE...

# Napadi iznutra

- iz sustava i korisnika koji su pod nadležnošću administratora
- autorizirani korisnici - **saboteri**
  - većinom slučajne greške, šteta nije zanemariva!
- zloupotreba **ovlasti** kod **administratora**
- djelatnici koji imaju pristup sustavu ali nisu zaduženi za uslugu

# Napadi izvana

- kriminalne ili terorističke organizacije
- obavještajne službe
- komercijalna poduzeća (industrijska špijunaža)
- istražiteljske agencije
- državne agencije
- hackeri i *script-kiddies*

# Načini napada

- elektronički
  - neautorizirani pristup sustavu
    - problemi konfiguracije, pogrešne ovlasti za pristup
  - računalni virusi
  - privremeno uskraćivanje usluge
- ostale metode
  - krađa opreme, provale
  - prijevara: društveni inženjerинг
  - plansko postavljanje agenata unutar sustava
  - poricanje korištenja usluga i izbjegavanje obaveza
  - krivotvorenje dopuštenja za pristup sustavu
  - krađa lozinki ili kartica za pristup

# Osnovni sigurnosni zahtjevi

- povjerljivost (*confidentiality*)
  - cjelovitost, integritet (*integrity*)
  - raspoloživost (*availability*)
- 
- autentifikacija (*authentification*)
  - neporecivost (*nonrepudiation*)
  - kontrola pristupa (*access control*)
- 
- ranjivi:
    - sklopolje
    - programska podrška
    - podaci



CIA

# Cjelovitost

- cilj IS: zaštititi podatke od neovlaštenog brisanja, mijenjanja ili bilo kakve manipulacije bez prethodne autorizacije
- načela uspostave kontrole cjelovitosti su:
  - dodjela samo nužnih prava pristupa (engl. *need-to-know basis*)
    - ograničavanjem prava pristupa povećava se razina sigurnosti ali i složenost samog sustava
    - pronaći zadovoljavajuću razinu sigurnosti i praktične produktivnosti
  - odvajanje dužnosti (engl. *separation of duties*)
    - raspodjela odgovornosti nad ključnim dijelovima procesa na barem dvije fizičke osobe sa istim privilegijama
  - rotacija dužnosti (engl. *rotation of duties*)
    - rotacija zaposlenika na sličnu dužnost povećava internu razinu kontrole i smanjuje mogućnost napada

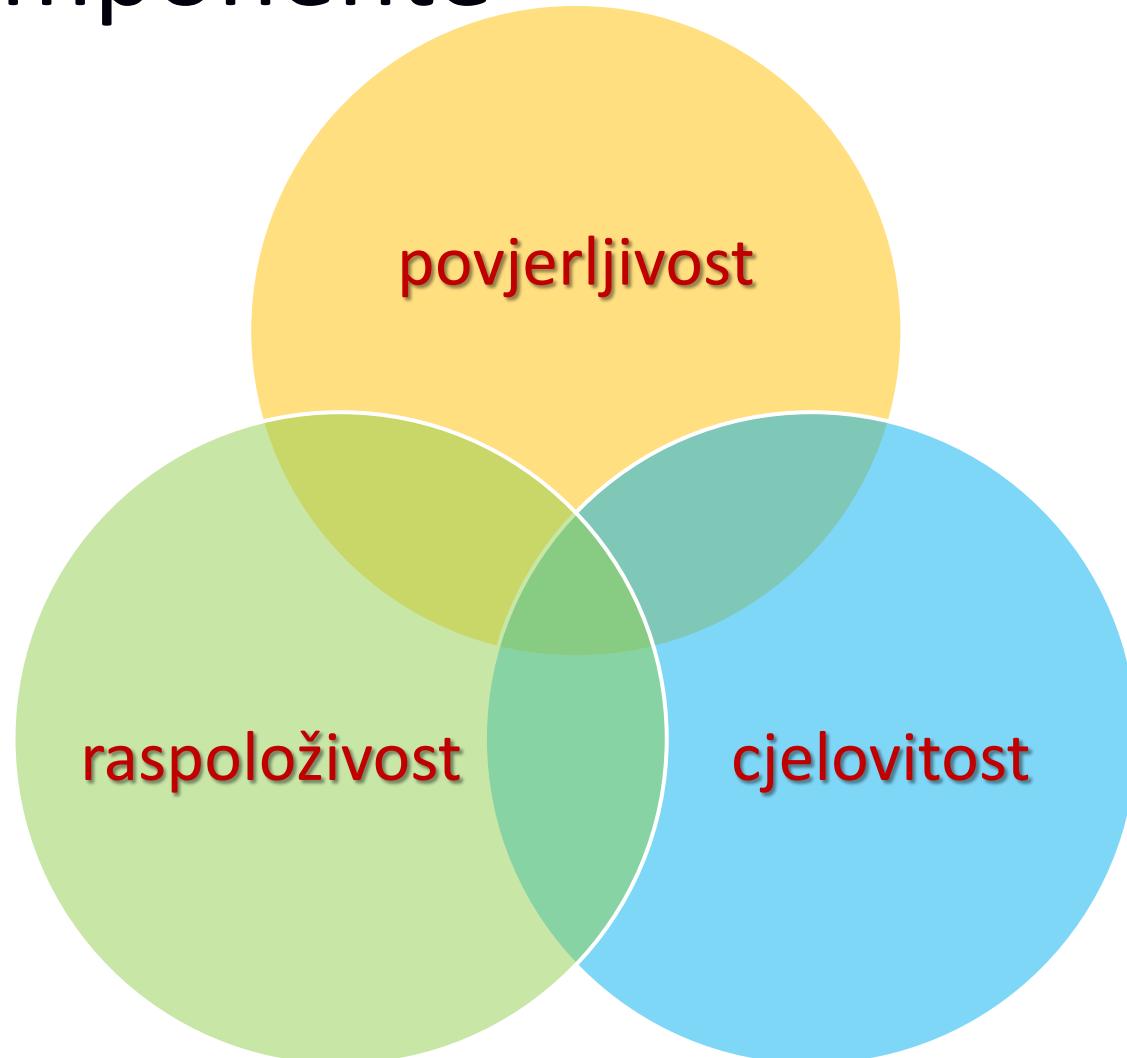
# Povjerljivost

- cilj IS-a: identifikacija i autentifikacija korisnika
- najčešće prijetnje povjerljivosti :
  - hakiranje - preuzimanje kontrole iskorištavanjem sigurnosnih slabosti sustava
  - maskiranje - pristup resursima koristeći neovlašteno pribavljene tuđe autorizacijske podatke
  - nezaštićeno preuzimanje datoteka - prijenos datoteka u okruženje dostupno neovlaštenim korisnicima
  - trojanski konji
- napadi se odnose i na narušavanje svojstva cjelovitosti
- još: tajnost, privatnost

# Raspoloživost

- cilj IS-a: dostupnost tražene usluge u promatranom trenutku ili u definiranom vremenskom rasponu usprkos mogućim neočekivanim i nepredvidljivim događajima
- smanjenje ili uskraćivanje raspoloživosti radi:
  - napada uskraćivanjem usluge (engl. Denial of Service)
  - gubitak sposobnosti obrade podataka kao rezultat prirodnih katastrofa ili nedostatka temeljnih potreba sustava (struja, hlađenje)

# Odnos 3 komponente



# Autentifikacija

- autentifikacija:
  - potvrda autentičnosti korisnika
    - odgovarajuće metode primjenjuju se ovisno o aplikaciji i uslugama koje ih koriste
  - razlika: identifikacija – autentifikacija
- neporecivost:
  - sudionici ne mogu odbiti ili poreći akciju u kojoj su sudjelovali, npr. slanje i primanje informacija
- kontrola pristupa:
  - ograničavanje pristupa informacijama i ograničavanje provođenja akcija

# Ranjivosti sustava

- **malware (*malicious software*)**
  - softver kojem je svrha infiltracija i oštećenje računala
    - *spyware* i *adware* (uglavnom napad na privatnost)
    - *virusi*
    - *crvi*
    - *trojanci*
    - *dialeri*
- **lažne poruke (*hoax*)**
  - poruke neistinitog sadržaja
- društveni inženjerинг
- društvene mreže
- mobilni uređaji

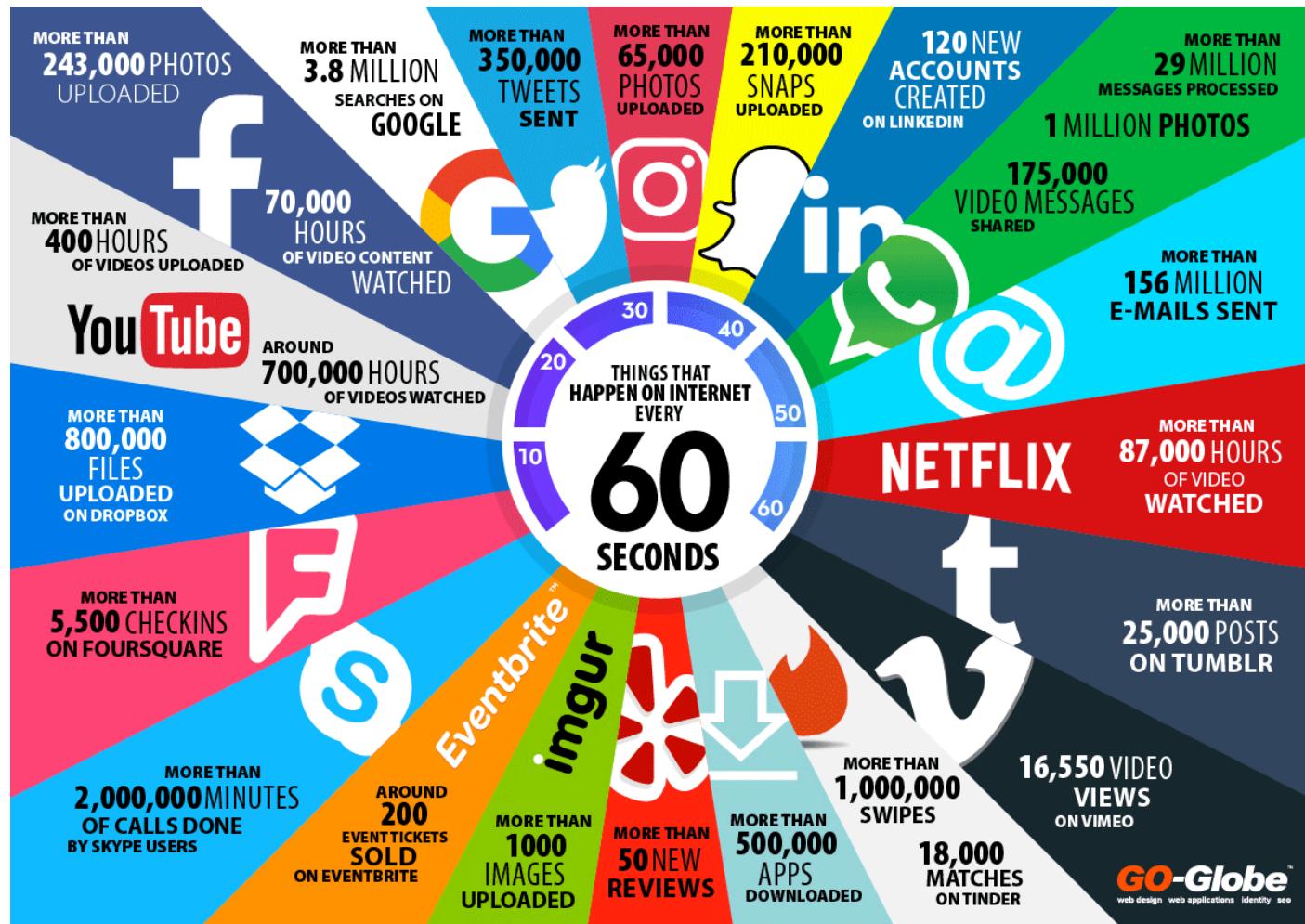
# Pojam sigurnosti

- sigurnost mreža, usluga i aplikacija – bitna za stvaranje povjerenja
  - sposobnost informacijskog sustava da se odupre neočekivanim događajima i neprijateljskim akcijama
  - mogući ciljevi napada:
    - raspoloživost
    - vjerodostojnost
    - integritet
    - povjerljivost
- ranjivost je posljedica sigurnosne slabosti i nedostataka
  - napadač to iskorištava za kompromitaciju i neovlašten pristup
- rješenje: nadzor i kontrola ranjivosti



# Zašto su podaci važni?

# Podaci na Internetu?

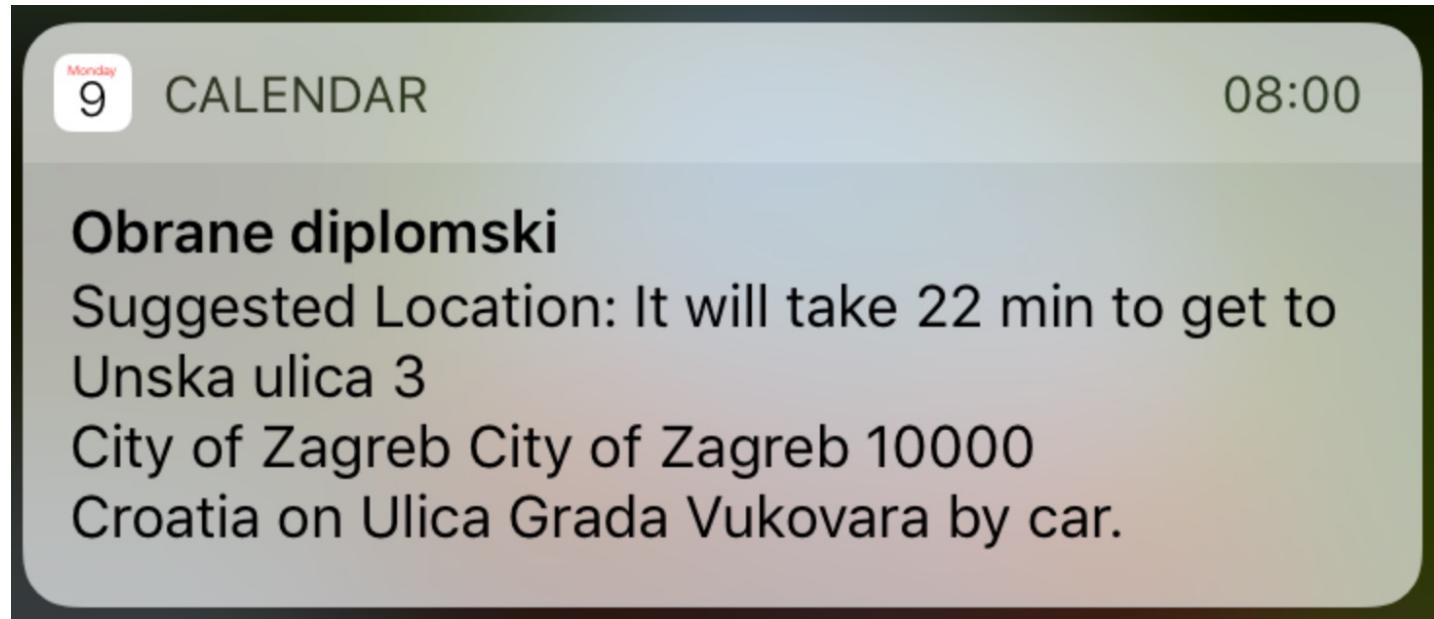


# „Pametno”

- Pametne tehnologije?
  - pametni telefoni (cca 2007)
    - iPhone, Android...
  - pametne usluge
    - mobilne aplikacije, web aplikacije/usluge -> aplikacije/usluge “u oblaku”
  - pametne kuće
    - električna energija, grijanje/hlađenje, uređaji, nadzor
  - pametna industrija
    - optimizacije procesa, logistike, proizvodnje -> Industrija 4.0
  - pametni gradovi
    - nadzor, upravljanje, ekologija...
- što je zajedničko svim “pametnim” tehnologijama?
  - podaci o korisniku pametne tehnologije!

} Internet stvari (IoT)  
machine-to-machine  
(m2m)

# „Pametno” - primjer



# Problem s podacima

- Usluga mora obrađivati osobne podatke korisnika kako bi korsnici bili "zadovoljni" uslugom
  - jednostavnost, uporabljivost
- Problemi:
  - što sve usluge skupljaju o korisnicima?
  - kako usluge čuvaju osobne podatke korisnika?
  - za što sve usluge koriste osobne podatke korisnika?
  - gdje su podaci koje smo nekada ostavili "na Internetu"?
  - "pravo na zaborav"?

# Osobni podaci

- Što bi trebali smatrati osobnim podatkom?
  - npr. podaci kreditne kartice – tradicionalno
    - Slanje kopija kartica telefaksom?
    - Krađa podataka kreditnih kartica je očekivana pa se i bolje štiti
- Razmisliti o...
  - podaci za kontakt (e-mail, telefon, mobitel, adresa...)
  - osobni podaci (spol, bračno stanje, dob...)
  - podaci na društvenim mrežama
  - podaci na mobitelu (lokacija, kontakti, poruke, kretanje...)
  - podaci o kreditnim karticama (naravno)
- Kakve se sve “priče” mogu smisliti poznavanjem samo nekih od ovih podataka?
  - *Have I been PWNed?* <https://haveibeenpwned.com/>

# Možemo li se uopće zaštititi?

- ako želimo koristiti napredne, “pametne”, tehnologije i usluge
  - moramo se djelomično odreći privatnosti
  - moramo djelomično vjerovati davateljima usluga
  - moramo biti svjesni što se može dogoditi ako napadač dobije pristup našim podacima

**"If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It"**

Eric Schmidt

Primjer: sigurnost alata za video konferencije

# COVID-19 i rast korisnika...

- ZOOM: 300 milijuna sudionika dnevno (travanj2020)
  - 10 milijuna u prosincu 2019.
- MSTeams: 75 milijuna sudionika dnevno (travanj 2020)
  - +70% od prosinca 2019.
- Ostali: npr. Webex oko 250.000 dnevno (travanj 2020)
- Dobar primjer:
  - kako sigurnost često nije u prvom (a ni u drugom?) planu
  - kako napadi rastu proporcionalno broju korisnika

# Zoom i ranjivosti (3/4/5 2020.)

- Zoom i Facebook SDK
  - Razmjena zbog funkcionalnosti „prijava putem Facebooka”
  - Nova verzija više ne podržava razmjenu podataka s Facebookom
- Zoom bombing
  - infiltracija napadača u videokonferencije drugih korisnika, uz neprimjerene poruke, prijetnje i ucjene
  - pozivi za videokonferencije bili javno dostupni, bez kontrole pristupa – naknadno uvedene „čekaonice”, lozinke, mogućnost prijave napadača (eng. Report a user)
  - kompleksniji meetingID – teže za nasumično pogađanje

# Zoom i ranjivosti (3/4/5 2020.)

- Zoom @Windows ranjivosti
  - krađa korisničkih podataka – hash lozinke – putem UNC-a
  - 0-day: *remote code execution* – kroz datoteke, bez upozorenja korisniku
- Šifriranje s kraja na kraj? - tek u srpnju 2020!
  - do tada moguće: lažne poruke, povjerljivost...
  - Problem: spajanje putem drugih mreža (npr. PSTN)
- Company Directory
  - automatsko dodavanje korisnika na listu kontakata ukoliko su pripadnici iste poslovne organizacije
  - pogrešne postavke Zooma - otkrivanje podataka drugih korisnika na istoj domeni (e-mail, profili, slanje zahtjeva)

# Zoom i ranjivosti (3/4/5 2020.)

- Zoom i LinkedIn Sales Navigator
  - povezivanje korisnika Zooma i korisnika LinkedIna i prikupljanje podataka u svrhu marketinga
- zWarDial
  - alat za automatiziranu pretragu meeting ID oznaka, nekada moguće pristupiti bez lozinke
- Snimke video poziva
  - Jednostavan algoritam imenovanja snimki pohranjenih u nezaštićenom "oblaku"
- 500,000 Zoom korisničkih računa na dark webu!

# Zakonska regulativa

(Republika Hrvatska i EU)

# KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA

- Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21)
- Glava XXV. Članci 266 – 273
  - **Neovlašteni pristup**
  - Ometanje rada računalnog sustava
  - Oštećenje računalnih podataka
  - Neovlašteno presretanje računalnih programa
  - Računalno krivotvorenje
  - Računalna prijevara
  - Zloupotreba naprava
  - Teška kaznena djela protiv računalnih sustava, programa i podataka

# Kibernetička sigurnost

- EU Regulativa
  - Direktiva 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194) – Poznata pod nazivom „NIS Direktiva“
  - Svrha: Osigurati da zemlje EU-a budu pripravne i spremne na rješavanje kibernetičkih napada
- HR zakonodavstvo
  - Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)
  - Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/18)
  - Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njezinu provedbu (NN 108/15)

# Kritična infrastruktura

- EU Regulativa
  - Direktiva 2008/114/EZ o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (SL L 345)
  - Svrha: Identificirati europsku kritičnu infrastrukturu i poboljšati njenu zaštitu od svih vrsta prijetnji i opasnosti
- HR zakonodavstvo
  - Zakon o kritičnim infrastrukturama (NN 56/13)

# Elektroničko poslovanje

- EU Regulativa
  - Uredba(EU) 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (SL L 257) – Poznata pod nazivom „eIDAS Uredba“
  - Svrha: Povećati povjerenje u online usluge i elektroničku trgovinu te osigurati uzajamno priznavanje elektroničke identifikacije među članicama EU
- HR zakonodavstvo
  - Zakon o provedbi Uredbe (EU) 910/2014 (NN 62/17)

# Elektroničke komunikacije

- EU Regulativa
  - Direktiva (EU) 2018/1972 o Europskom zakoniku elektroničkih komunikacija (SL L 321)
  - Svrha: Reguliranje elektroničkih komunikacijskih mreža i usluga, povezane opreme i usluga, poboljšati suradnju na razini EU te potaknuti razvoj 5G i mreža velikog kapaciteta
- HR zakonodavstvo
  - Zakon o elektroničkim komunikacijama (NN [73/08](#), [90/11](#), [133/12](#), [80/13](#), [71/14](#), [72/17](#))

# Pristupačnost

- EU regulativa
  - Direktiva (EU) 2016/2102 Europskog parlamenta i Vijeća od 26. listopada 2016. o pristupačnosti internetskih stranica i mobilnih aplikacija tijela javnog sektora (SL L 327)
  - Svrha: Poboljšati pristupačnost internetskih stranica i mobilnih aplikacija tijela javnog sektora i omogućiti lakši pristup javnim uslugama, posebice osobama s invaliditetom.
- HR zakonodavstvo
  - Zakon o pristupačnosti mrežnih stranica i programske rješenja za pokretne uređaje tijela javnog sektora (NN 17/2019)

# Zaštita osobnih podataka

- EU regulativa
  - Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (SL L 119)
  - Svrha: Građanima omogućiti bolju kontrolu nad njihovim osobnim podatcima, a poduzećima olakšati korištenje i prenošenje osobnih podataka
- HR zakonodavstvo
  - Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)

# Pravo na pristup informacijama

- EU regulativa
  - Direktiva (EU) 2019/1024 o otvorenim podatcima i ponovnoj uporabi informacija javnog sektora (SL L 172)
  - Svrha: Olakšati pristup i korištenje informacija javnog sektora i državne uprave, ojačati podatkovno gospodarstvo EU i pospješiti razvoj umjetne inteligencije
- HR zakonodavstvo
  - Zakon o pravu na pristup informacijama (NN [25/13, 85/15](#))

# Zaštita klasificiranih podataka

- EU regulativa
  - Odluke Vijeća 2013/488/EU i 2015/444 o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a i njena (SL L 274, SL L 72)
    - Svrha: Zaštititi klasificirane podatke od neovlaštenog pristupa i otkrivanja
- HR zakonodavstvo
  - Zakon o tajnosti podataka(NN [79/07](#), [86/12](#))

# Zaštita poslovne tajne

- EU regulativa
  - Direktiva (EU) 2016/943 o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja (SL L 157)
  - Svrha: Zaštita od nezakonitog pribavljanja, korištenja i otkrivanja poslovnih tajni
- HR zakonodavstvo
  - Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti (NN 30/18)

# Zaštita autorskog prava i intelektualnog vlasništva

- EU regulativa
  - [Direktiva 2001/29/EZ o usklađivanju određenih aspekata autorskog i srodnih prava u informacijskom društvu](#) (SL L 167)
  - Direktiva 96/9/EZ o pravnoj zaštiti baza podataka (SL L 77)
  - Direktiva 2009/24/EZ o pravnoj zaštiti računalnih programa ((SL L 111)
  - Direktiva 2004/48/EZ o provedbi prava intelektualnog vlasništva (SL L 157)
  - Direktiva 2006/123/EZ o uslugama na unutarnjem tržištu (SL L 376)
  - Direktiva (EU) 2015/2436 Europskog parlamenta i Vijeća od 16. prosinca 2015. o usklađivanju zakonodavstava država članica o žigovima (SL L 336)
  - Svrha: Omogućujući zaštite autorskog prava intelektualnog vlasništva i potaknuti na suradnju među članicama EU
- HR zakonodavstvo
  - [Zakon o autorskom pravu i srodnim pravima](#) (NN 111/21)
  - Zakon o patentu (NN 16/20)
  - Zakon o žigu (NN 14/19)
  - Zakon o industrijskom dizajnu (NN [173/03](#), [54/05](#), [76/07](#), [30/09](#), [49/11](#), [46/18](#))
  - Zakon o naknadama u području intelektualnog vlasništva (NN 66/21)
  - Zakona o zastupanju u području prava industrijskog vlasništva (NN 54/05, 49/11, 54/13)



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost podatkovnog sloja



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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.

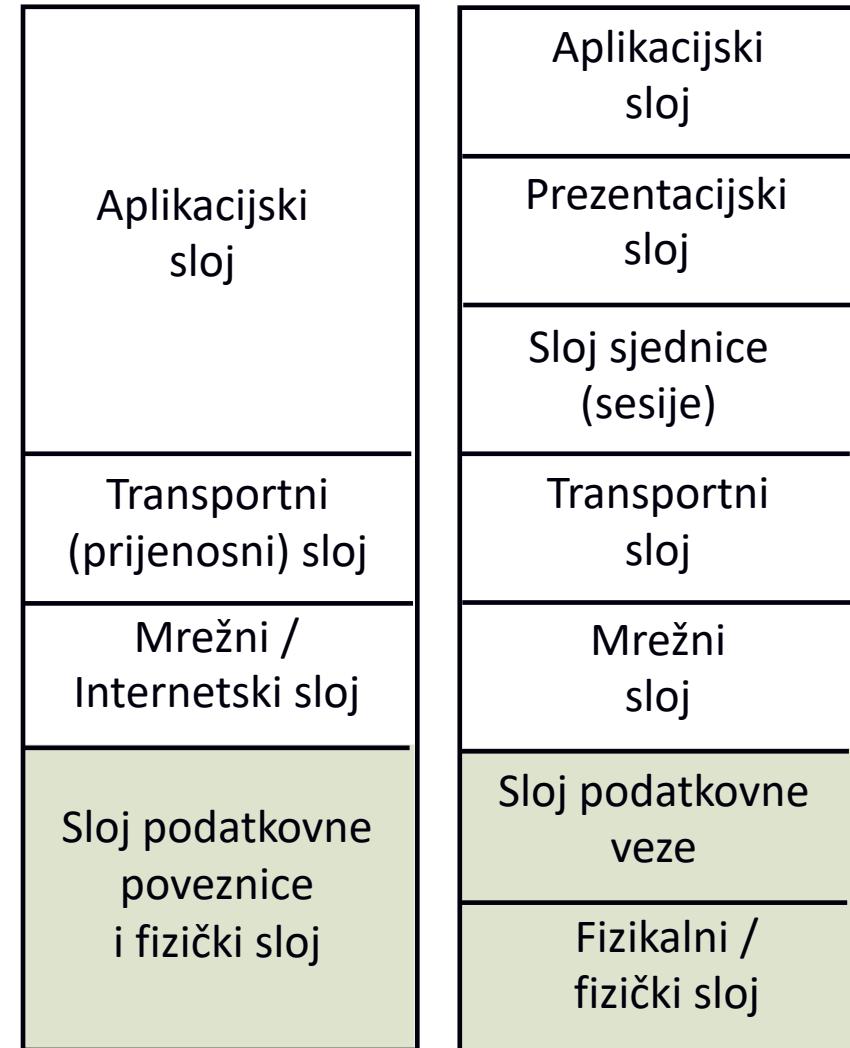
Tekst licencije preuzet je s <http://creativecommons.org/>.

# Sadržaj

- općenito o podatkovnom sloju
- sigurnost lokalnih mreža
- elementi lokalne mreže Ethernet
- ranjivosti
- zaštita mreže Ethernet
- osnovno o sigurnosti ostalih podatkovnih mreža

# Općenito o podatkovnom sloju

- drugi sloj ISO/OSI referentnog modela
- sve „ispod Interneta”
- zadaća
  - omogućiti komunikaciju dva direktno povezana računala/mrežna uređaja
- niz bitnih i manje bitnih protokola/tehnologija
- Ethernet, xDSL, 2G/2.5G/3G/4G/5G, POTS/ISDN, WiMax, FrameRelay, ATM



# Ethernet

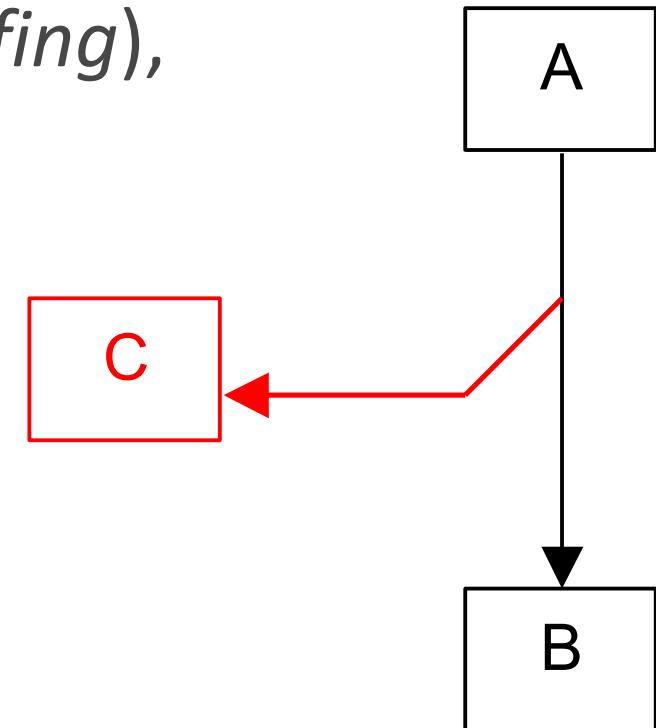
- izuzetno popularna mreža
  - u lokalnim mrežama gotovo da i nema alternative
- vrlo velik raspon brzina koje ta mreža pokriva
  - od 10 Mbps do 100 Gbps
  - razvoj 400 Gbps i planovi/potreba za Tbps brzinama
- u žičnoj (bakar i optika) i bežičnoj varijanti
  - žični i bežični Ethernet se na fizičkom sloju potpuno razlikuju, na podatkovnom manje (iz perspektive mrežnog sloja su svi identični)
- dodatna upotreba
  - povezivanje lokacija na području grada (Metro Ethernet)
  - industrijski Ethernet

# Elementi mreže Ethernet

- ključne komponente žične mreže Ethernet
  - preklopniци (komutatori, engl. switch) (prije: koncentratori, engl. hub)
  - kabeli
    - vertikalno i horizontalno kabliranje
    - bakrene žice i optika
- bežični Ethernet se temelji na pristupnim točkama
  - uglavnom se spaja na žični Ethernet
- dodatno se na mreži nalaze i drugi uređaji koji na prvi pogled ne izgledaju kao preklopniци i/ili računala
  - VoIP telefoni

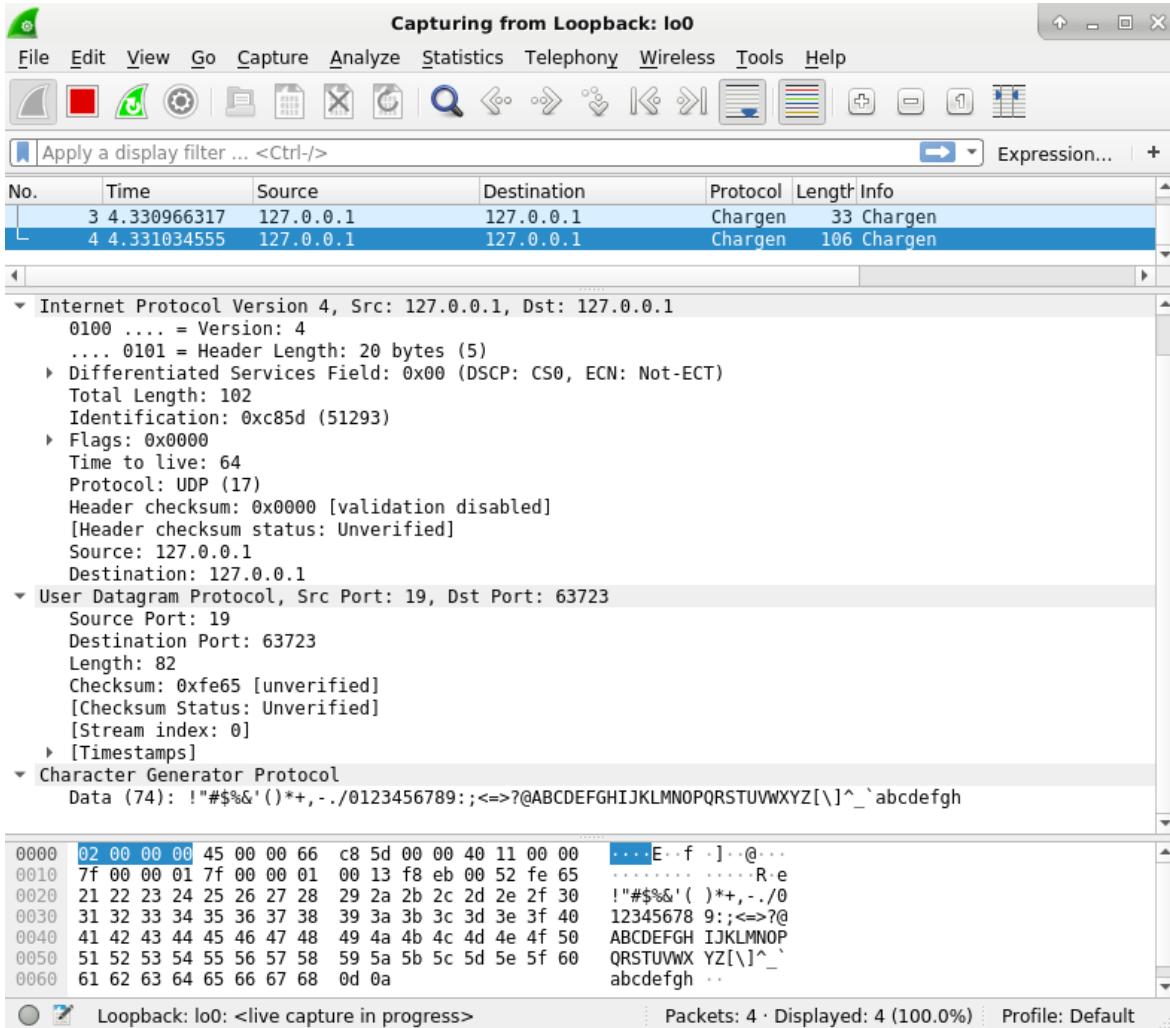
# Presretanje, prisluškivanje

- Presretanje (*interception*), prisluškivanje (*evesdropping*), njuškanje mreže (*network sniffing*), prisluškivanje na vodu (*wiretapping*)
  - elektronička komunikacija se presreće i preuzima informacija
  - Potencijalne štete
    - Neovlaštena uporaba podataka
    - Potencijalno narušavanje privatnosti
- Zakonski regulirano presretanje (*lawfull interception*)



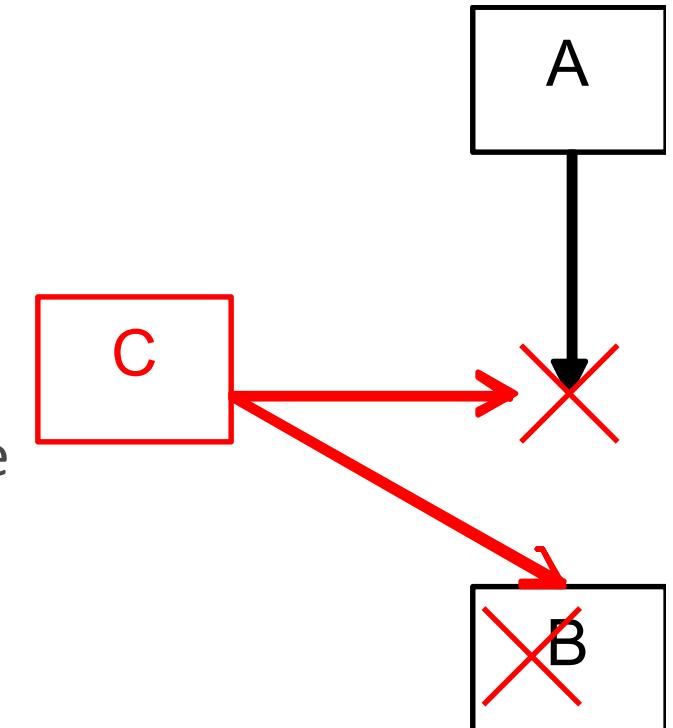
# Network sniffing

- temelj za mnoge napade
  - napadač postavlja svoju mrežnu karticu u promiskuitetni način rada - vidi sav promet na tom segmentu
  - mrežna kartica predaje sve pristigle pakete IP sloju
  - mnogi protokoli prenose autentifikacijske podatke u obliku čistog teksta => username/password itd.
- alati: Wireshark, tcpdump, ...



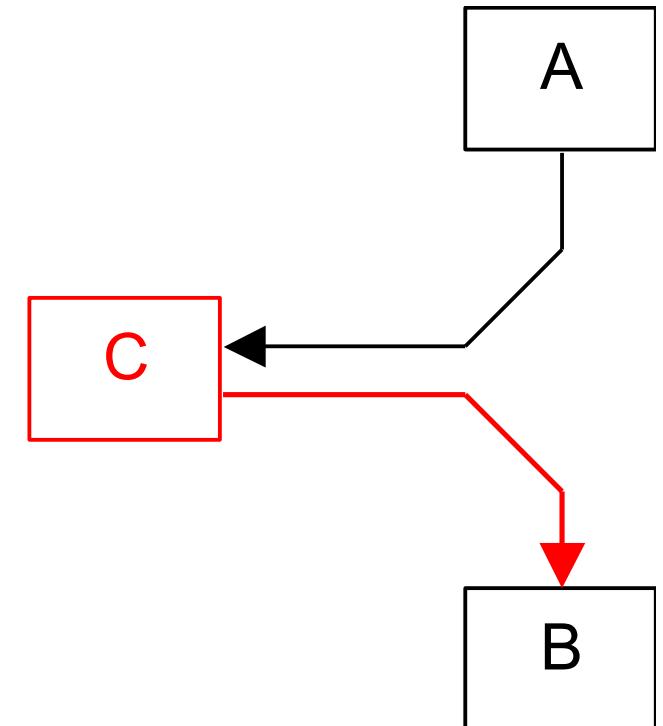
# Prekidanje, uskraćivanje

- **Prekidanje** (engl. interruption)
  - prekidanje normalnog tijeka komunikacije, usluge ili aplikacije
- **Uskraćivanje usluge** (engl. denial of service)
  - onemogućavanje usluge izazivanjem preopterećenja mreže ili umreženog sustava



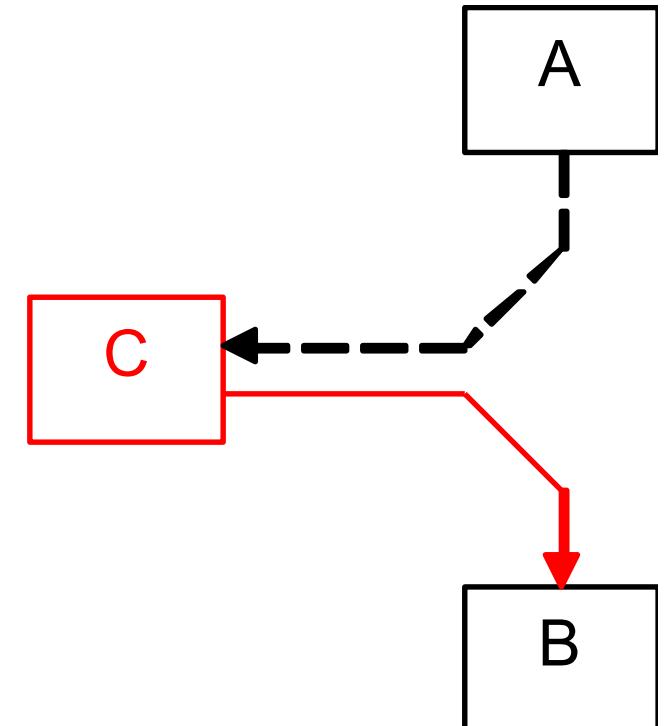
# Promjena, kašnjenje

- Promjena (engl. modification, tampering)
  - Promjena ili uništenje informacije
  - Kašnjenje može izazvati isti učinak – podatak postaje nevažan



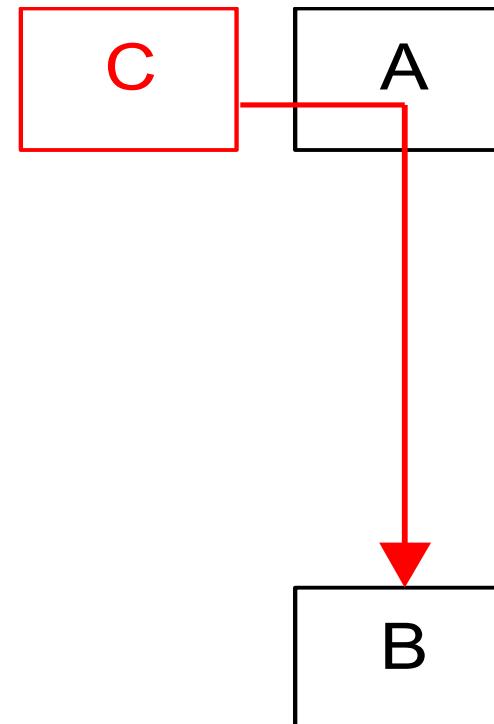
# Umetanje, ponavljanje

- Umetanje, ubacivanje (engl. fabrication)
  - Ubacivanje zlonamjerne informacije
- Ponavljanje (engl. replay)
  - Ubacivanje informacije prethodno preuzete presretanjem



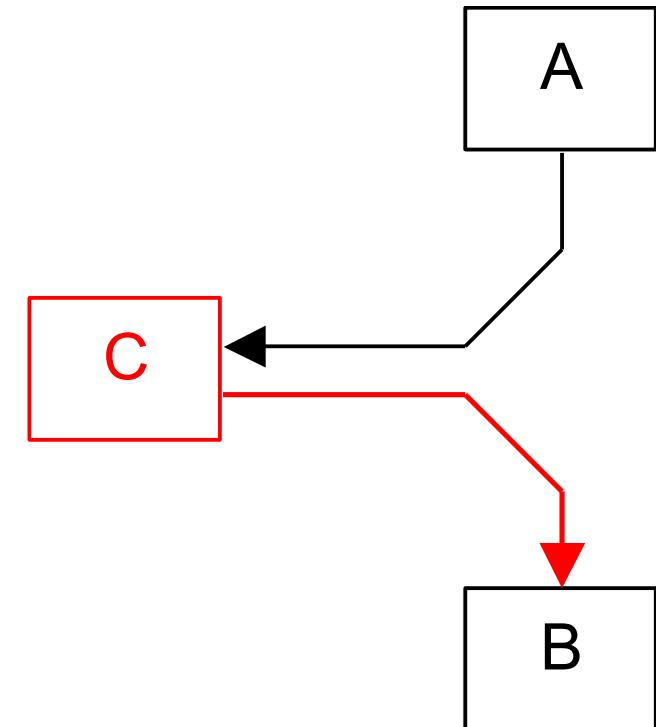
# Lažno predstavljanje

- Lažno predstavljanje
  - Maskiranje (engl. masquerade)
  - Lažno predstavljanje (engl. impersonation)
  - Preuzimanje identiteta i uloge korisnika



# „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
- Najbolji položaj za napadača i najgori za branitelja



# Cilj napadača u slučaju mreže Ethernet

- neovlašteni pristup mreži
  - manipulacija prometom na mreži
- sve to je vrlo vjerojatno tek međukorak u nekom složenijem napadu
  - pristupiti lokalnoj mreži ili preuzeti kontrolu nad njom i ne činiti ništa nema baš nekog smisla(!)
- neke mogućnosti zloupotrebe pristupa Ethernet mreži
  - preuzimanje kontrole nad preklopnicima
  - enumeracija, praćenje prometa i aktivnosti na mreži
  - pretvaranje da se radi o nekome drugome

# Preduvjeti napada na Ethernet mrežu

- računalo s odgovarajućim ovlastima na mreži
- pristup mreži
  - fizički pristup nekoj komponenti mreže
    - žicama, mrežnim priključnicama, preklopnicima (+konzola)
    - omogućavaju direktni pristup mreži
  - pristup putem Interneta
  - pristup preklopnicima preko usmjernika
  - pristup nekom računalu već spojenom na mrežu
    - trojanci
  - udaljeni rad (VNC, RDP, TeamViewer, ssh)

# Fizički pristup lokalnoj mreži (1)

- manipulacija žica
  - bakrene vodiče (UTP CATn) je vrlo jednostavno manipulirati
  - optiku je puno teže manipulirati, ali ne i nemoguće
  - posebno problematično vertikalno povezivanje (*backbone*)
- pristup mrežnim utičnicama
  - priključivanje vlastitih računala
  - posebno problematične utičnice koje se nalaze u javnim prostorima!

# Fizički pristup lokalnoj mreži (2)

- pristup preklopnicima
  - direktno spajanje na preklopnike i pristup linkovima za vertikalno povezivanje
  - zamjena preklopnika i manipulacija njegovim OS-om
  - pristup konzoli
    - telnet(!), web(!), ssh
  - jednostavni DoS napadi

# Prisluškivanje prometa (1)

- najjednostavnije je prisluškivati promet (engl. sniffing)
  - pasivni napad
  - mrežne kartice prihvaćaju samo određeni promet
  - s odgovarajućim ovlastima to možemo promijeniti
    - tzv. *promiscuous mode*
- što se postiže na taj način?
  - praćenje prometa na mreži
  - dohvati povjerljivih informacija (npr. lozinke)
- koliko je to teško?
  - izuzetno jednostavno!
  - alati npr. tcpdump, wireshark, ngrep,...

# Prisluškivanje prometa (2) - primjer

- promet snimljen tijekom prijave na HTTP Web stranicu i rekonstruiran u jednostavni tekst

Stream Content

```
GET /~sgros/os/ HTTP/1.1
Host: www.zemris.fer.hr
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.12) Gecko/20101027 Fedora/3.6.12-1.fc14
Firefox/3.6.12
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Authorization: Basic c2dyb3M6cGVybw==

HTTP/1.1 200 OK
Date: Mon, 22 Nov 2010 11:23:22 GMT
Server: Apache/2.2.3 (CentOS)
Content-Length: 1796
Connection: close
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /~sgros/os</title>
</head>
<body>
```

Find Save As Print Entire conversation (2405 bytes)  ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

# Prisluškivanje prometa (3)

- problem za napadača
  - ethernet mreža je preklapana mreža
  - ne stiže sav promet do svih mrežnih kartica
  - krajnja računala promet vide samo pod određenim uvjetima
- "rješenje": zlorabiti lošu implementaciju
  - ograničen spremnik MAC adresa
  - primjerice HP ProCurve 2600 serija

	horizontal surface mounting only	horizontal surface mounting o
Performance		
Latency	< 13.3 µs (LIFO)	< 12 µs (LIFO)
Throughput	up to 10.1 million pps	up to 10.1 million pps
Routing/Switching capacity	13.6 Gbps	13.6 Gbps
MAC address table size	8000 entries	8000 entries
Environment		

# Prisluškivanje prometa (4)

- uobičajen rad preklopnika
  - uči položaj MAC adresa na temelju izvorišne adrese
  - zaboravlja nakon nekog vremena naučene adrese
- napad na preklopnik u kojemu se generira mnoštvo lažnih MAC adresa
  - u trenutku kad se MAC tablica prepuni, preklopnik se degenerira u koncentrator (moguće pratiti sav promet)
- zaštita
  - ograničenje broja MAC adresa po portu
  - fiksiranje nekih kritičnijih MAC adresa

# Sigurnost protokola ARP

- protokol ARP služi za povezivanje IP i MAC adresa
  - vrlo jednostavan i nezaštićen protokol
- ideja napada – slati lažirane ARP odgovore
- mogućnosti koje napadač ima na raspolaganju
  - otimanje komunikacije (engl. hijacking)
  - praćenje i izmjena prometa koji prolazi između dvije strane koje komuniciraju
  - pretvarati se da smo izvor informacija
  - uskraćivanje usluge

# Ranjivost protokola ARP

- ARP - protokol za pretvaranje 32 bitnih IP adresa u 48 bitne Ethernet (MAC) adrese
- ako računalo A želi poslati IP datagram računalu B ili usmjeritelju u lokalnoj mreži, tada ono mora znati njegovu MAC adresu
- A šalje broadcast ARP zahtjev na mrežu (uključujući svoje preslikavanje)
- B odgovara računalu A, porukom ARP odziv
- preslikavanje se lokalno pohranjuje u svakom računalu u ARP cache:  
\$ arp –an

# Ranjivost protokola ARP

tip hardvera (2 okteta)	tip protokola (2 okteta)	
duljina hw adrese (1 oktet)	duljina prot. adr. (1 oktet)	kod operacije (2 okteta)
hardverska (ethernet, MAC) adresa pošiljatelja (6 okteta)		
IP adresa pošiljatelja (4 okteta)		
hardverska (ethernet, MAC) adresa primatelja / cilja (6 okteta)		
ciljna IP adresa (4 okteta)		

- ovisno o tipu poruke, određena polja su prazna:
  - za ARP: odredišna HW adresa,
  - za RARP: sve osim izvorišne HW adrese.

# Napad na ARP

- ARP nema ugrađene mehanizme autentifikacije
- moguće je poslati odgovor prije pravog računala te vratiti lažno preslikavanje adresa (IP/HW)
- lažni ARP odgovori mogu se koristiti za spremanje krivih ARP preslikavanja na računalu kome su upućeni
- ARP poruke mogu se slati kontinuirano kako bi se (lažni) podaci zadržali u *cacheu*

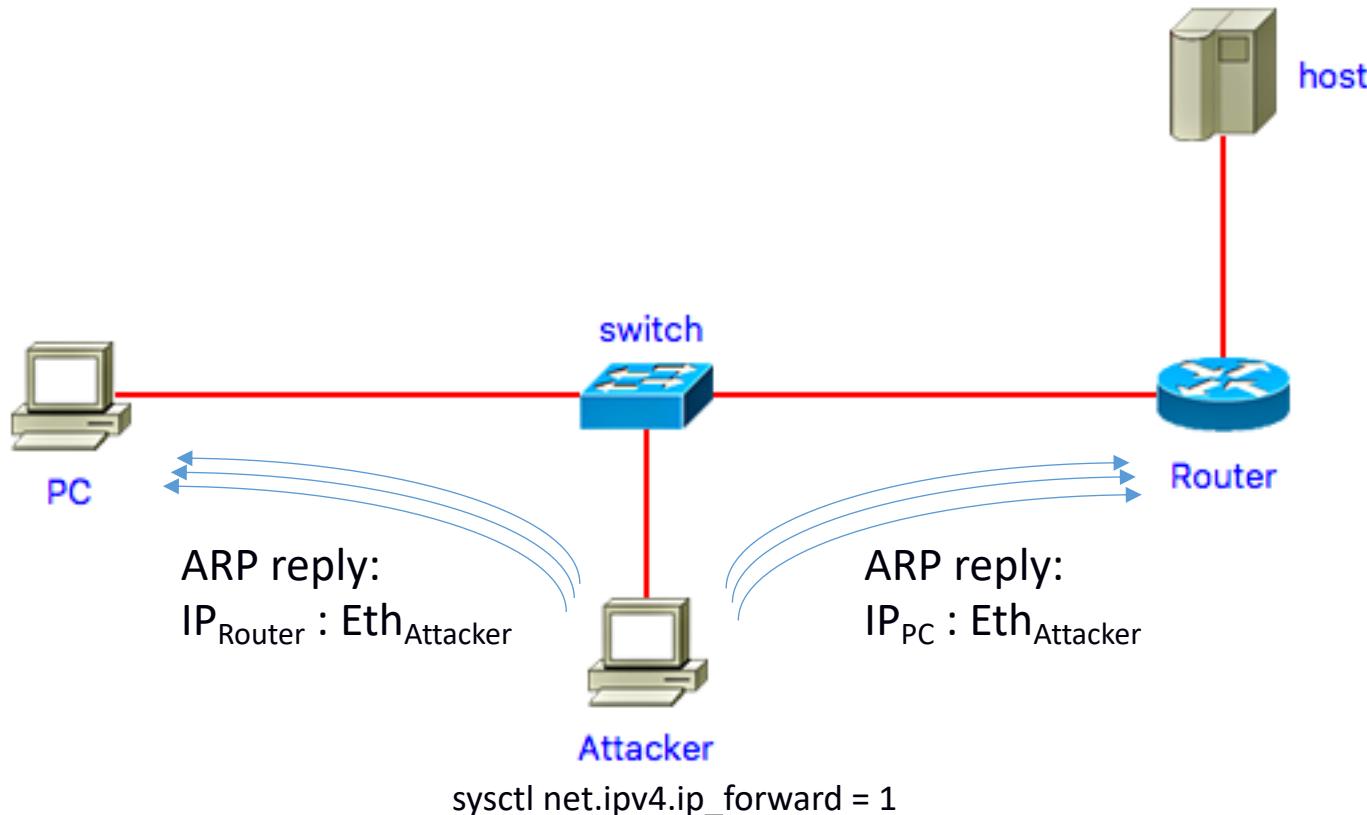
# Napadi mogući iskorištavanjem protokola ARP

- slanje nepostojećih MAC adresa za IP adrese
  - nemogućnost komunikacije - uskraćivanje usluge (DoS)
- ubacivanje između lokalnog usmjernika/poslužitelja i žrtve
  - napadač može pratiti svu komunikaciju i snimati tajne podatke
  - utjecati na komunikaciju
- skeniranje mreže u potrazi za aktivnim uređajima
  - arping, nmap
- vrlo poznat alat ettercap za provođenje napada
  - slobodno dostupan na Internetu
  - sadrži i GUI te omogućava „point-and-click“ napade

# Napad na ARP

- Cilj:
  - Prisluškivanje prometa (preklopnik, komutator (switch) prosljeđuje ethernet okvire između mrežnih sučelja na temelju ethernet adrese odredišta)
  - Prekidanje: lažno preslikavanje IP adrese usmjeritelja na nepostojeću MAC adresu (DoS napad)
  - Promjena
  - Ometanje
- alati: arpoison, ettercap, dsniff, parasite

# Napad na ARP



# Napad na ARP - otkrivanje i zaštita

- ako je preuzimanje bilo uspješno, malo je vjerojatno da će korisnici napadnutog računala išta primijetiti
- najjednostavniji način: ispis ARP cachea
  - ako se MAC adresa od određene IP adrese promijenila napadačevo računalo se identificira s pomoću te MAC adrese te po mogućnosti fizički odspaja s mreže
- može se detektirati s nekog trećeg računala, na kojem se njuška mreža i traže lažni ARP odzivi
- u slučaju DoS napada, lagano je ustanoviti da nešto nije u redu

# Napad na ARP - zaštita

- ako postoji neobično ponašanje u mreži korisno je pogledati ARP cache
- korištenje hardvera koji će učiniti takve napade nemogućima ili više vidljivima
  - korištenje komutatora, *switch*, s mogućnošću “zaključavanja” priključaka (*port security*)
- onemogućavanje ARP-a i njegova ručna konfiguracija

# Zaštita od manipulacija korištenjem protokola ARP

- ograničenja manipulacije protokolom ARP
  - radi isključivo unutar jedne difuzne (engl. broadcast) domene
  - napadnuto računalo mora već imati zapis MAC-IP za računalo s kojim mu želimo prekinuti komunikaciju
- zaštita
  - staticki zapisi
  - praćenje ARP prometa
  - preklopnići mogu pratiti promjene u suradnji s DHCP poslužiteljem/protokolom

# IPv6 – NDP

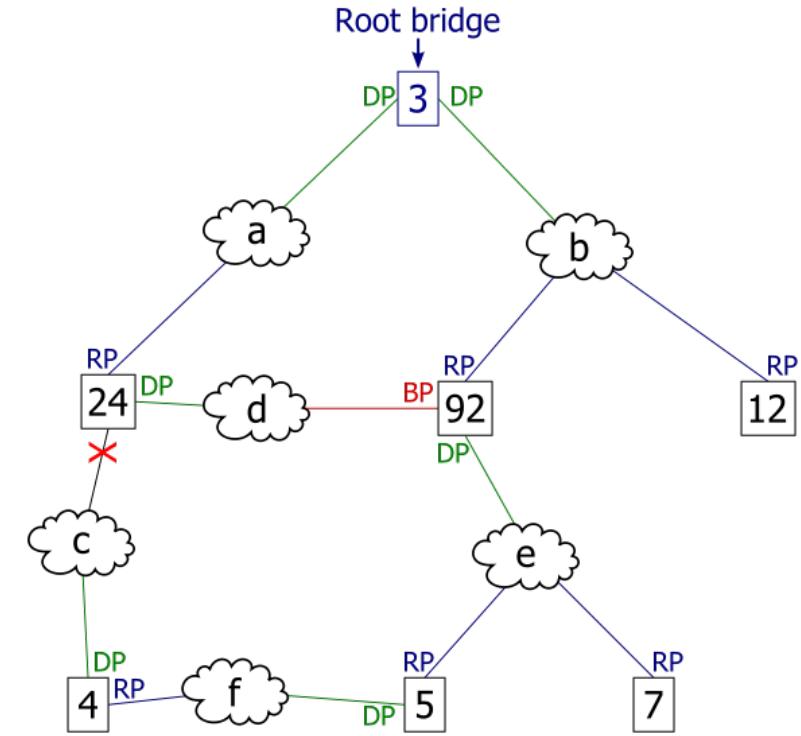
- ARP je zamijenjen protokolom NDP - "Neighbor Discovery Protocol" (ICMPv6)
  - nema autentifikacije (kao ni ARP)
  - staticki zapisi prepisuju se dinamičkim
  - ARP Spoofing ---> NDP Spoofing
- dostupni alati
  - "THC – The Hacker Choice": Parasit6, Fakerouter6, ...

# IPv6 – SEND

- protokol SEND - "Secure Neighbor Discovery"
  - NDP + kriptografska zaštita
- CGA - Cryptographically Generated Addresses (RFC 3972)
  - svaki uređaj ima par RSA ključeva (ne treba certifikat)
  - valjanost se djelomično provjerava
  - zaštita od NDP spoofinga, onemogućen spoofing valjane CGA adrese
- nedostaci:
  - usmjeritelji moraju obavljati puno kriptografskih operacija (dio se može odraditi unaprijed)
  - potencijalni DoS jer usmjeritelj mora čuvati puno stanja
  - dostupno na Unixoidnim sustavima (Windows ?)

# Protokol R/STP

- Ethernet mreža je izuzetno automatizirana
  - učenje MAC adresa
  - redundantni putovi (petlje)
    - mogu u potpunosti zagušiti mrežu
- protokoli Spanning Tree Protocol (STP, 802.1D) i Rapid Spanning Tree Protocol (RSTP, 802.1w)
  - koriste algoritam razapinjućeg stabla (engl. spanning tree):
    - razmjenjuju BPDU podatkovne jedinice (engl. bridge protocol data unit)
    - parametri: identifikatori i težine, premosnika i pristupa
  - cilj: ostvariti topologiju stabla s najjačim preklopnicima u centru



# Ranjivosti protokola R/STP (1)

- faze protokola
  - odabir korijenskog premosnika (engl. root bridge)
  - odabir korijenskih pristupa (engl. root ports)
  - odabir odabralih pristupa (engl. designated ports)
  - promjena stanja pristupa
- stanja pristupa
  - onemogućen (engl. disabled)
  - blokirajući – samo prihvata BPDU-ove (20s)
  - osluškuje – prihvata i prosljeđuje BPDU-ove (15s)
  - učenje – tablica prosljeđivanja se izgrađuje (15s)
  - prosljeđuje – podatkovni promet se prosljeđuje

# Ranjivosti protokola R/STP (2)

- namjerna modifikacija topologije
  - radi uskraćivanja usluge (stalno u procesu otkrivanja topologije)
  - radi preusmjeravanja prometa
- izvršenje napada je relativno jednostavno
  - unutar Linux operacijskog sustava nalazi se implementiran protokol STP
  - vrlo je jednostavno napraviti prenosnik koristeći operacijski sustav Linux
- problem (za napadača!)
  - velika količina prometa

# Ranjivosti protokola R/STP (3)

- zaštita
  - zabraniti protokol STP na priključnicama gdje su krajne stanice
  - Cisco terminologija: **BPDU Guard**
- zabraniti pristupima da postanu korijenski pristupi
  - Cisco terminologija: **Root Guard**

# Implementacija virtualnih LAN mreža

- IEEE 802.1Q, (Dot1q): virtual LANs (VLANs)
- vrlo popularna metoda za izolaciju prometa
- dodatno 32-bitno polje u zaglavlju; između izvođačne MAC adrese i polja EtherType
- komunikacija između VLAN-ova isključivo preko usmjernika/vatrogaza
- jedan preklopnik poslužuje više virtualnih LAN mreža
  - VLAN za goste (samo pristup Internetu), VLAN za knjigovodstvo, poslužitelje, ...
- preklopnići se međusobno povezuju „trunkovima”
- svaki pristup preklopnika može
  - biti isključivo u jednom VLAN-u
  - biti u više VLAN-ova
  - biti u više VLAN-ova s podrazumijevanim VLAN-om

# Napadi na VLAN mreže (1)

- problem s automatskim povezivanjem više VLAN-ova (engl. dynamic trunking); napad „switch spoofing“
  - dodavanje računala koje se predstavlja kao preklopnik
- dvostruko označavanje (engl. double tagging)
  - napadač šalje okvir s dvije oznake
  - prvi preklopnik uklanja prvu oznaku i šalje okvir prema drugom preklopniku putem *trunk* porta (po prvom VLAN-u)
  - drugi preklopnik vidi drugu oznaku VLAN-a

# Napadi na VLAN mreže (2)

- kako bi napad dvostrukog označavanja radio potrebno je
  - napadač i žrtva moraju biti na različitim preklopcima
  - napadač mora znati MAC adresu žrtve
  - napadač ima isti VLAN ID kao i podrazumijevani na trunku
- zaštita
  - ne koristiti nativni VLAN
- potencijalno VLAN preskakanje uz pomoć usmjernika
  - usmjerniku se šalje okvir s njegovom MAC adresom i odredišnom adresom žrtve u drugom VLAN-u

# Dinamičko konfiguriranje računala

- dodjela IP adresa nekad:
  - Reverse ARP, RARP - samo IP adresa, bez adresa DNS poslužitelja
  - i Bootstrap Protocol, BOOTP (dodatni podaci za bootanje preko mreže)
- Dynamic Host Configuration Protocol, DHCP
  - kompatibilan s BOOTP, koristi iste portove
  - može efikasno dodjeljivati adrese iz skupa raspoloživih adresa
  - IP adresa može biti fiksirana uz MAC adresu
  - standardno na svim operacijskim sustavima (za IPv4)
  - ograničen na jednu podmrežu ali usmjeritelji mogu podržavati "relay" agente
- DHCPv6

# Protokol DHCP

- Služi za automatsku dodjelu adresa i mrežnih parametara
  - Klijent šalje svima na mreži poruku DHCPDISCOVER
    - Klijent u tom trenutku ne zna adresu
  - Poslužitelji odgovaraju klijentu s porukom DHCPOFFER
  - Klijent odabire poslužitelj i šalje svima DHCPREQUEST
  - Poslužitelj odgovara s DHCPACK
- Fiksiranje adresa na temelju MAC adrese radi kontrole pristupa
  - Moguće i na temelju identifikatora

# Protokol DHCP

- klijent šalje UDP zahtjev na broadcast adresu 255.255.255.255 port 67
- DHCP poslužitelj šalje ponudu adrese
  - u pravilu treba biti jedan DHCP poslužitelj u podmreži
  - u ponudi se standardno nalazi puno dodatnih podataka: *default router*, adrese DNS poslužitelja

# Problemi protokola DHCP

- Nema nikakve zaštite poruka
  - Bilo tko može slati i primati DHCP poruke
- Lažni DHCP poslužitelji na mreži
  - Napadi uskraćivanja usluga
  - Preusmjeravanje prometa
- Bilo koji klijent može zatražiti parametre
  - Lako se zaobilazi MAC/ID zaštita
  - Moguće iscrpljivanje svih raspoloživih adresa („DHCP Starvation attack“)

# Ostali mogući problemi u lokalnoj mreži Ethernet

- protokol **SNMP**
  - davanje informacija o preklopniku
  - mogućnost promjene podataka u preklopniku
- protokoli **LLDP** (Link Layer Discovery Protocol) i CDP (Cisco Discovery Protocol)
  - davanje podataka o topologiji mreže
- udaljen pristup preklopniku (telnet/ssh/Web)
  - napadi pogađanjem lozinke
  - korištenje zasebnog VLAN-a

# Zaštita lokalne mreže Ethernet (1)

- fizička infrastruktura mora biti zaštićena
  - vertikalno kabliranje u kanalicama
  - horizontalno kabliranje posebno zaštićeno
  - mrežne utičnice koje se dulje ne koriste moraju biti isključene
  - preklopnići u zaključanim ormarićima pod odgovarajućim nadzorom
- koristiti upravljive preklopnike
  - ispravna autentikacija pristupa upravljačkom modulu
  - izoliranje prometa po VLAN-ovima
  - autentikacija prije pristupa mreži (802.1x)
  - ograničenje broja MAC adresa po pristupu
  - isključiti upravljačke protokole na pristupima gdje se ne očekuju drugi preklopnići
  - neupravljeni preklopnići ne nude nikakvu zaštitu
    - treba ih izbjegavati!

# Zaštita lokalne mreže Ethernet (2)

- računala i aplikacije
  - korisnici na računalima bez administratorskih ovlasti
    - spriječena instalacija programa i manipuliranje podatkovnim slojem
  - antivirusni alati radi zaštite od malicioznog koda
  - strogi nadzor i kontrola udaljenog pristupa
  - korištenje kriptiranja radi zaštite integriteta, tajnosti i autentičnosti podataka (SSL, IPsec)

# Ostali protokoli podatkovne veze

- ADSL se uzima za pristup Internetu
  - ekonomski najisplativija opcija za surfanje
  - moguć vektor ulaska u zaštićenu mrežu
- primjer ranjivosti
  - D-Link „backdoor“
- krivo podešeni ADSL usmjernici mogu propustiti napadače u lokalnu mrežu
- modemski pristup
  - danas se vrlo rijetko koriste
  - potencijalna opasnost od njihova otkrivanja i ulaska u mrežu



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

Bežične mreže



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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/>.

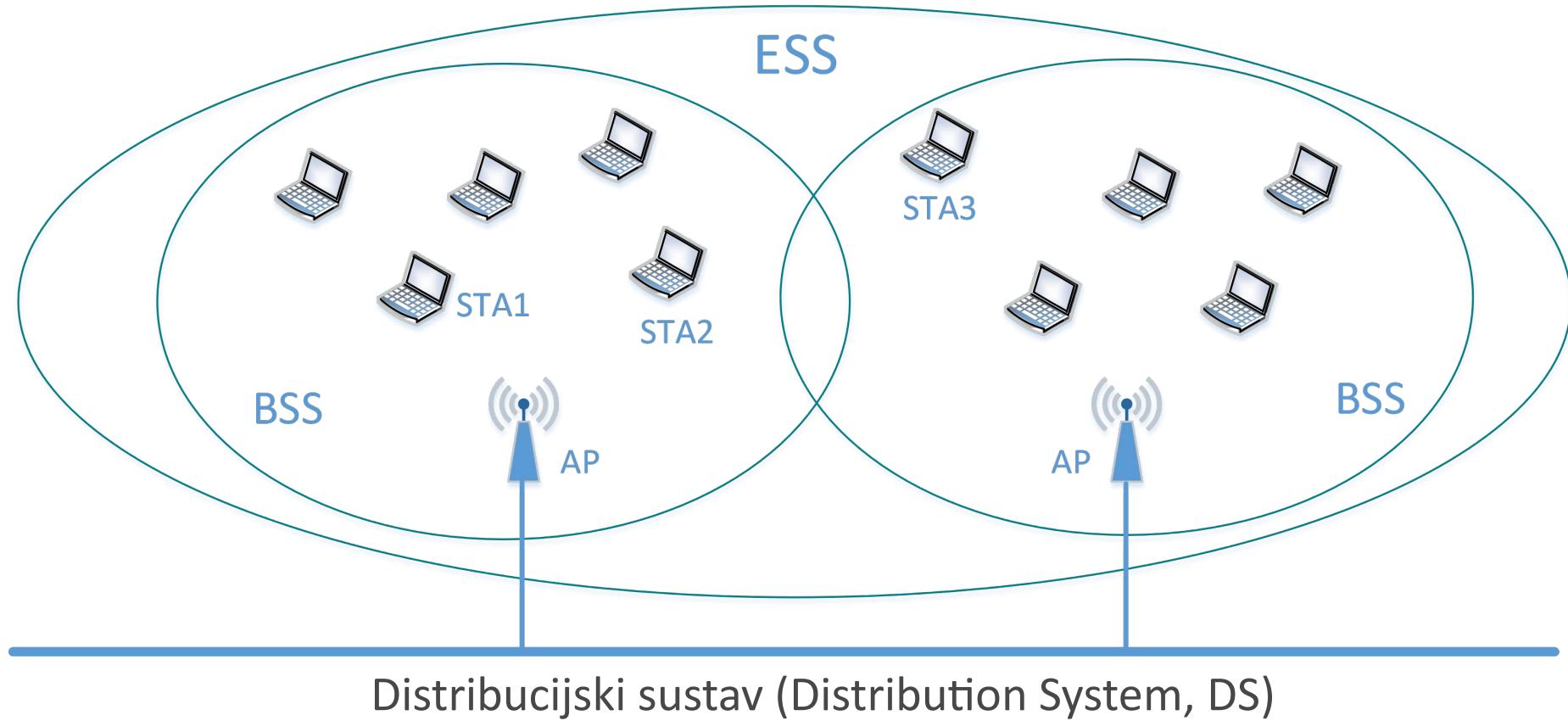
# Sadržaj

- osnovno o bežičnim mrežama
- karakteristike Wi-Fi/802.11 bežičnih mreža
- 802.1x i EAP
- napadi na WPS, WPA i PSK/WPA Enterprise
- sigurnost u mobilnim mrežama

# Osnovna svojstva bežičnih mreža

- bežične mreže koriste elektromagnetske valove za prijenos podataka
  - po prirodi je vrlo teško ograničiti pristup mediju
- mnoštvo je različitih bežičnih mreža
  - u ovom dijelu bavit ćemo se sa 802.11
  - kasnije u predmetu bit će riječi o Bluetooth i o mobilnim mrežama iz perspektive mobilnih uređaja
- dva osnovna načina rada 802.11: ad-hoc i infrastrukturni
  - Ad-hoc (IBSS, Independent Basic Service Set) omogućava direktnu komunikaciju stanica
  - u infrastrukturnom načinu rada koristi se pristupna točka (AP) preko koje svi komuniciraju

# Arhitektura 802.11 u infrastrukturnom načinu



- STA – *station, stanica*
- AP – *access point, pristupna točka*

# Neki dodatni pojmovi

- pojedina pristupna točka identificirana je s **BSSID** parametrom (engl. Basic Service Set Identifier)
  - najčešće jedna od MAC adresa pristupne točke
- skup pristupnih točaka identificiran je **ESSID**-om (ili kraće SSID-om) (engl. Extended Service Set ID)
  - identifikacijski niz maks. duljine 32 znaka
  - nije namijenjen kontroli pristupa; objavljuje se u tzv. Beacon upravljačkim okvirima
- zbog karakteristika medija sigurnost bežičnih mreža značajno se temelji na kriptografiji!

# BSS - Basic Service Set

- jedna pristupna točka (AP), oglašava SSID (kao naziv mreže za taj BSS)
- klijenti se spajaju na AP
- fizička dostupnost signala: BSA (Basic Service Area)
- AP je u pravilu „uplinkom” spojen na Ethernet

# ESS - Extended Service Set

- više pristupnih točaka (Access Points) koje imaju isti SSID (a različite BSSID) povezano na komutator (switch)
- korisnik može prelaziti iz područja signala jednog AP u drugi bez raskidanja komunikacije (*roaming*)

# 802.11 porodica bežičnih mreža

- lokalna bežična mreža temeljena na protokolu Ethernet

IEEE standard	Max brzina	Frekvencija	Napomena
<b>802.11 (1997)</b>	2 Mbps	2.4 GHz	Inicijalna verzija koja se više ne koristi
<b>802.11a (1999)</b>	54 Mbps	5 GHz	Nekompatibilna s b i g standardima
<b>802.11b (1999)</b>	11 Mbps	2.4 GHz	Često korištena tehnologija zbog starije opreme
<b>802.11g (2003)</b>	54 Mbps	2.4 GHz	Često korištena tehnologija zbog starije opreme
<b>802.11n (2009)</b>	600 Mbps	2.4 GHz / 5 GHz	Najčešće korištena varijanta
<b>802.11ac (2014)</b>	7 Gbps	5 GHz	Najnoviji, sve više u upotrebi
<b>802.11ax (2021)</b>	9.6 Gbps	2.4 / 5 / 6 GHz	„Wi-Fi 6“ (6. verzija standarda 802.11)

# Protokoli za sigurnost bežičnih mreža (1)

- za sigurnost bežičnih mreža definirani su WEP, WPA, WPA2 i WPA3
  - WPA (Wi-Fi Protected Access) je komercijalni i zaštićeni nazivi Wi-Fi udruge
  - IEEE definira 802.11i normu i u sklopu nje RSN („Robust Security Network“) i TSN („Transitional Security Network“)
- WEP definiran 1999. godine
  - školski primjer kako ne upotrebljavati kriptografiju
- WPA uveden 2003. godine kao privremena mjera
  - baziran na draftu 802.11i specifikacije
  - bilo je nužno podržati postojeću opremu koja je omogućavala WEP
- WPA2 definiran 2004. godine

# Protokoli za sigurnost bežičnih mreža (2)

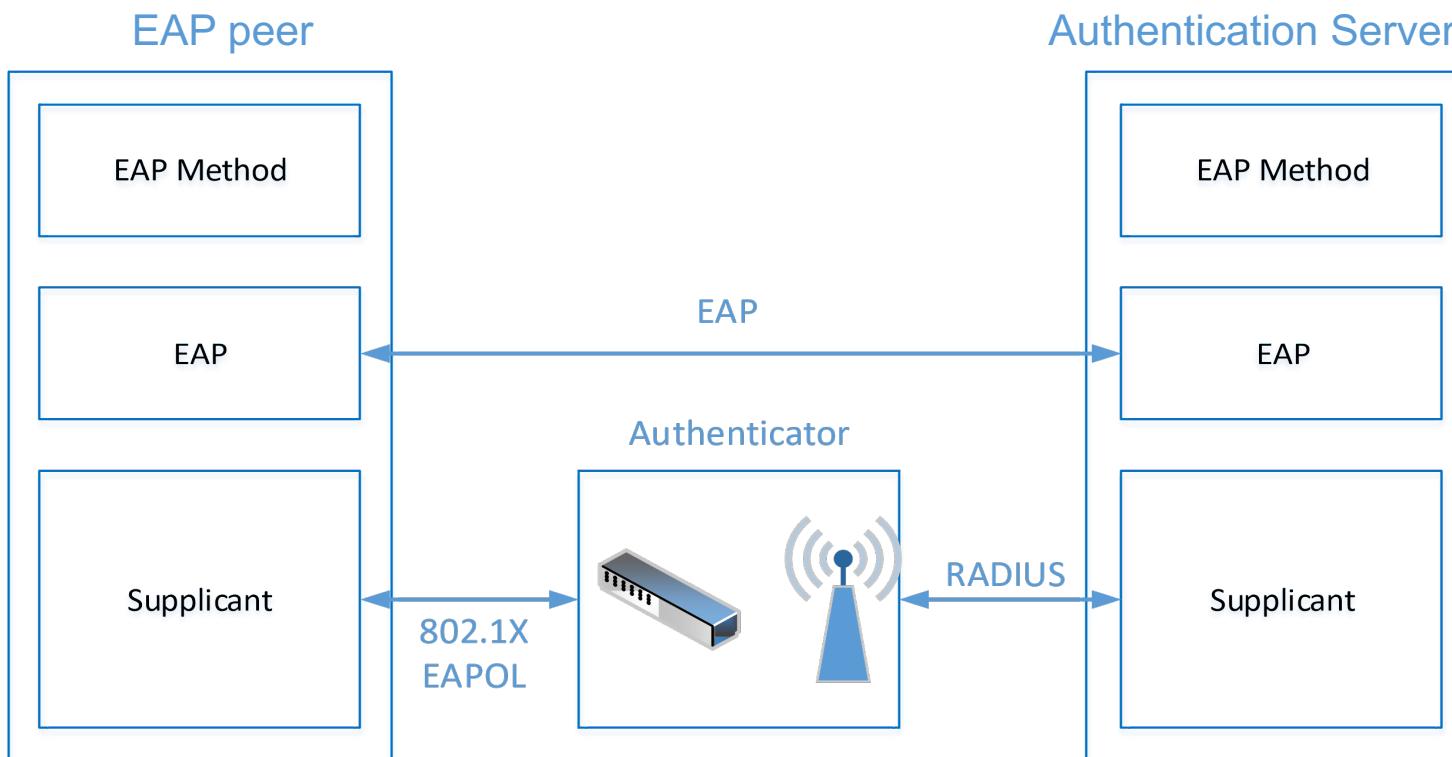
- WPA3 definiran u 7. mjesecu 2018. godine
  - poboljšana zaštita prilikom korištenja nedovoljno kompleksnih lozinki
    - Simultaneous Authentication of Equals (SAE)
  - dijeljena tajna u WPA3-Personal se više ne može jednostavno pogađati
  - uklonjeni kripto algoritmi koji se smatraju nesigurnima
  - uvedena zaštita upravljačkih okvira (Protected Management Frames, PMF)
  - uvodi ključeve veličine 192-bit u WPA Enterprise inačicu
    - dodatne zaštite za prijenos osjetljivih informacija u okruženjima kao što su financijske ili vladine institucije.
  - Wi-Fi CERTIFIED Easy Connect – spajanje na mrežu jednostavnih uređaja (IoT uređaji) upotrebom nekog složenijeg uređaja (primjerice, mobilnog telefona)
    - zamjena za WPS

# Kontrola pristupa bežičnoj mreži

- WPA/WPA2/WPA3 PSK
  - PSK – pre-shared key, dijeljena tajna
  - autentifikacija se temelji na dijeljenoj tajni veličine 8-63 ASCII ispisiva znaka
  - prednosti
    - jednostavna za postavljanje
  - nedostatci
    - u slučaju odlaska zaposlenika dijeljena tajna se mora mijenjati na svim uređajima
    - efektivno se radi o lozinci što znači da se mogu provoditi napadi koji se provode na njih
- WPA/WPA2/WPA3 Enterprise
  - centralizirana autentifikacija koju obavlja poseban poslužitelj (Radius)

# Arhitektura autentifikacije temeljene na EAP-u

- koristi se isključivo u WPA[23] Enterprise varijanti
  - potrebno je imati poseban autentifikacijski poslužitelj (Radius ili Diametar)



# EAP i 802.1x

- EAP: Extensible Authentication Protocol
- generički sustav mrežne autentifikacije (RFC3748)
- definira četiri tipa poruka: request, response, success, failure
  - ne definira kako se poruke prenose niti konkretnе metode autentifikacije
- dodatno se definiraju autentifikacijske metode
  - ima ih preko 40, standardnih i nestandardnih
  - neke metode su slabe, neke omogućavaju autentifikaciju samo klijenta, a neke jake i omogućavaju autentifikaciju i klijenta i poslužitelja
- za prijenos EAP poruka preko Etherneta u 802.1x-2010 je definiran protokol EAPOL
  - pokriva niz različitih mreža, ne samo 802.11

# Radius - Remote Authentication Dial-In User Service

- mrežni protokol za centralizirani AAA (authentication, authorization, accounting) za korisnike koji pristupaju i koriste mrežne usluge
- model klijent/poslužitelj (u pravilu UDP, može i TCP)
- „back-end“ za autentifikaciju 802.1X
- korisnik (ili uređaj) šalje NAS poslužitelju (Network Access Server) zahtjev za pristup određenom mrežnom resursu korištenjem svojih pristupnih vjerodajnica (*access credentials*)
  - šalje se nekim protokolom podatkovne veze, na primjer PPP (Point-to-Point Protocol) ako se radi o "dialup" ili xDLS pružatelju usluge ili se koristi HTTPS post kroz web forme

# Radius

(2)

- komunikacija NAS i Radius poslužitelja treba biti dodatno zaštićena na primjer IPsec tunelom
  - lozinka je zaštićena dijeljenom tajnom i MD5 algoritmom
- RADIUS poslužitelj provjerava informacije korištenjem autentifikacijskih shema tipa PAP, CHAP ili EAP
- verificira se identitet korisnika, adresa, broj telefona, stanje računa, dozvole za pristup mrežnim uslugama
- korisnički podaci: lokalne datoteke (nekad), danas SQL, LDAP, Active Directory, ...

# Radius

(3)

- NAS šalje RADIUS poslužitelju poruku "Access Request"
  - sadrži pristupne vjerodajnice, tipično u obliku username/password ili korisničkog certifikata
  - dodatno se mogu nalaziti podaci o korisniku poznati NAS-u (mrežna adresa, broj telefona, podaci o fizičkom priključku)
- RADIUS poslužitelj odgovara:
  - Access Reject
  - Access Challenge (dodata lozinka, PIN, token, kartica) ili uspostava sigurnog tunela između korisnika i Radius poslužitelja
  - Access Accept

# Radius

(4)

- RADIUSaaS - Radius as a service
  - jednostavna i sigurna autentikacija za pristup mrežnim resursima
  - autentifikacija se temelji na klijentskim certifikatima
  - provjera opozvanih certifikata (OCSP)
  - generiranje konfiguracijskih profila
- Diameter
  - nadogradnja Radiusa, nije direktno kompatibilan
  - podrška za TCP i SCTP
  - pregovaranje mogućnosti
  - definirani mehanizmi za "failover"
  - mogućnost proširenja i nadogradnji
  - zaštita na transportnom sloju (TLS ili IPsec)

# Fizički sloj

- na fizičkom sloju definiraju se radio karakteristike
  - frekvencije, snaga, modulacije
- koristi se nelicencirani spektar 2.4 GHz i 5 GHz (6 GHz)
  - smetnje od drugih uređaja
- oblikom i razmještajem antena te snagom može se utjecati na pokrivenost
  - to ne znači da napadač ne može koristiti specijalnu opremu kako bi pristupio bežičnoj mreži s veće udaljenosti

# Vrste okvira i njihova zaštita

- u 802.11 bežičnim mrežama upotrebljavaju se tri vrste okvira:
  - podatkovni okviri – prenose korisničke podatke
  - upravljački okvir – upravljanje MAC-om
    - uspostavljanje asocijacija, reasocijacija, odspajanje, autentifikacija, beacon...
  - kontrolni okviri – upravljanje pristupom mediju
    - RTS, CTS, ACK, ...
- samo podatkovni okviri su kriptografski zaštićeni
  - norma 802.11w ratificirana 2009. godine omogućava zaštitu upravljačkih okvira
    - nije dostupno u svoj opremi
    - nije moguće zaštiti sve okvire (npr. Beacon), odnosno općenito sve koji se koriste prije prijave

# Napadi uskraćivanjem usluge

- RF ometanje (engl. RF jamming)
  - Queensland Attack (kontinuirano slanje jakog signala)
- virtualno ometanje (engl. Virtual jamming)
  - manipulacija RTS/CTS okvirima
- lažiran zahtjev za odspajanjem (engl. spoofed disconnect)
- Connection request flooding

# Napadi na kriptografiju

- WEP: školski primjer krive upotrebe kriptografije
  - uz pomoć gotovih alata (aircrack-ng) vrlo jednostavno je moguće doći do dijeljene tajne (potrebno je snimiti oko 50 k okvira)
  - nakon toga moguće je pristupiti mreži bez ikakvih problema
- WPA ima određenih problema
  - algoritam za zaštitu integriteta, Michael, nije dovoljno jak. U prosjeku nakon  $2^{28}$  pokušaja moguće je lažirati sadržaj poruke
  - kad se detektira krivi MIC (message integrity check) AP prepostavlja da je u pitanju aktivni napad i:
    - obavlja bilježenje sigurnosnog incidenta, blokira stanicu u slučaju 2 pogreške u 60s, mijenja PTK i GTK, blokira port
- WPA2 ima ranjivost KRACK (Key Reinstallation Attack)
  - <https://www.krackattacks.com>

# Nekriptografski napadi na WPA i WPA2

- WPA PSK ranjiv na pogađanje dijeljene tajne
- uz pomoć deautentifikacijskih napada moguće snimiti autentikaciju
- potom off-line pogađanje lozinki
  - na CPU, rješenja za GPU, korištenje Cloud usluge
- PSK je moguće otkriti i kompromitiranjem klijenata
- PSK omogućava spajanje na mrežu, ali ne i dešifriranje snimljenog prometa
  - potrebno je znati PTK (engl. pairwise transit key)

# Napadi na WPA2 Enterprise

- ranjivost ovisi o konkretnoj upotrijebljenoj EAP metodi
  - u RFC4017 definirane preporuke za EAP metode koje se koriste u bežičnim mrežama
- EAP-MD5, EAP-LEAP
  - podložni pogađanju lozinke, ne omogućava međusobnu autentifikaciju (MITM)
  - mora ih se koristiti sa nekakvom dodatnom zaštitom
- EAP-TLS, EAP-TTLS
  - sigurni, ali je potencijalni problem neodgovarajuće rukovanje certifikatima

# iOS Wi-Fi poruka „weak security”

- WPA koristi TKIP (Temporal Key Integrity Protocol)
  - ne smatra se sigurnim od 2009.
- WPA2 koristi CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
  - sigurniji, temelji se na AES
- napad na mrežu WPA + TKIP:
  - neki klijent mora biti spojen
  - izvede se deautentifikacija i dohvaća razmjena ključeva („four-way handshake”)
  - ugrađeno u aircrack-ng, pretraga rječnika dok se ne pronađe ključ
- WPA2
  - „deauthentication” okviri nisu šifrirani
  - DoS napad (ne može se spriječiti)
  - Rogue access point (Evil Twin Attack)

# WPS - Wi-Fi Protected Setup

- jednostavan mehanizam za konfiguriranje „sigurne” bežične mreže
  - za autentifikaciju pristupne točke i klijenta
- olakšava podešavanje WPA PSK zaštite
  - korisnik na računalu upiše 8-znamenkasti PIN zapisan na kućnom usmjerniku
  - usmjernik pošalje dobru dijeljenu tajnu računalu i na dalje se upotrebljava WPA PSK
- ranjivost (u dizajnu) bitno ograničava prostor mogućih vrijednosti
  - „brute force” napad može otkriti PIN za 4-10 sati
  - neovisno o korištenom šifriranju
- problem je što se radi samo o 8 znamenkastom broju
  - gdje je zadnja znamenka kontrolna
  - i znamenke se prenose u grupama 4+3 pri čemu AP daje odgovor već nakon prve grupe
  - dakle, potrebno je samo 11000 pokušaja ( $10^4 + 10^3$ , umjesto inicijalno zamišljenih  $10^8$ )

# Neovlaštene i otvorene pristupne točke

- neovlaštene pristupne točke (engl. Rogue access points)
  - može ih postaviti neki djelatnik u želji da si olakša pristup mreži
  - pristupne točke dolaze u raznim formatima – postoje USB verzije koje se mogu priključiti na prijenosna/stolna računala
  - napadač koji se pokušava ubaciti u komunikaciju ili dohvatiti inicialnu razmjenu radi vjerodajnica
  - Evil Twin Attack, napadač doda AP s istim ESSID kao legitimna pristupna točka
- otvorene pristupne točke na javnim mjestima ili u kafićima
  - problematične jer mogu biti namjerno podmetnute
  - ako nisu podmetnute, na tim otvorenim mrežama može se nalaziti napadač vrebajući žrtve

# Neke preporuke za sigurnost bežičnih mreža

- ne koristiti ako nije nužno
- ako se mora koristiti
  - upotrebljavati WPA3 Personal ili Enterprise verzije ako je ikako moguće
  - koristiti složene lozinke koje nije jednostavno pogoditi
  - upotrebljavati WPA2 Enterprise verziju
  - u slučaju WPA2 Enterprise paziti na korištenje odgovarajućih EAP metoda
  - ne koristiti WPS
- Wi-Fi Protected Access® Security Considerations (May 2021)  
[https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security\\_Considerations\\_20210511.pdf](https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security_Considerations_20210511.pdf)



SVEUČILIŠTE U ZAGREBU



Diplomski studij

Ak. godina 2022./2023.

# Sigurnost komunikacija

Sigurnost mrežnog sloja



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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.

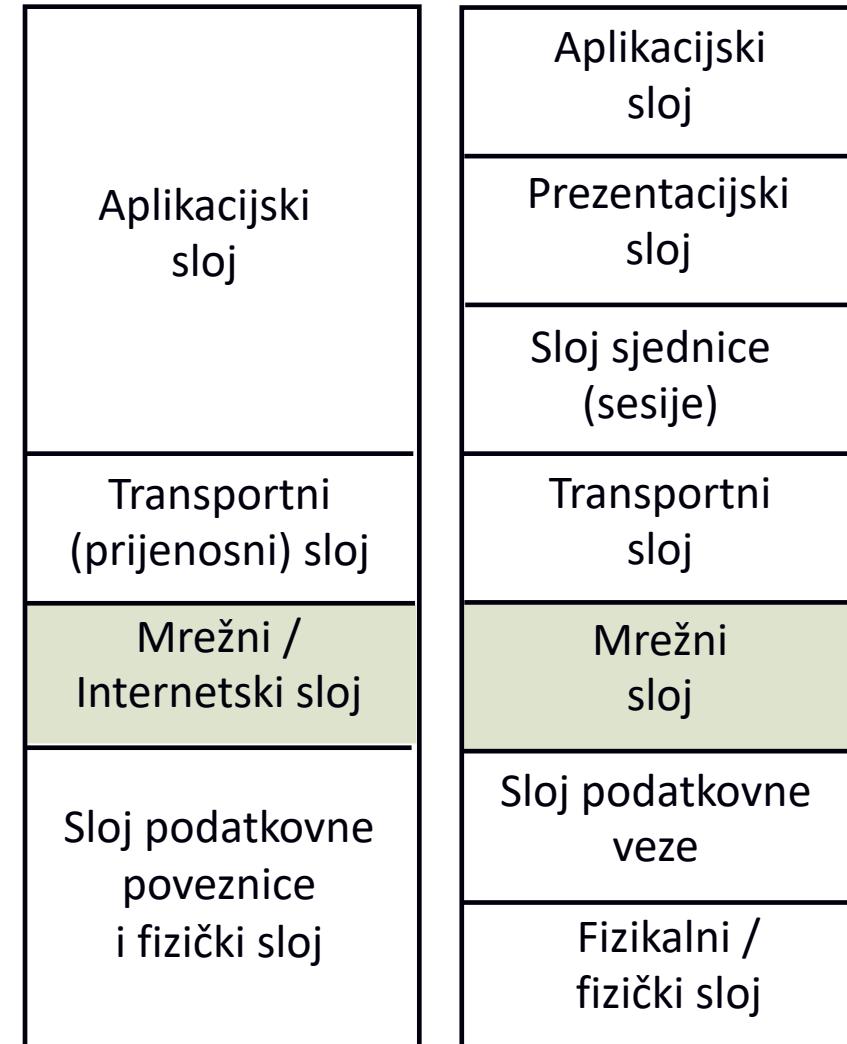
Tekst licencije preuzet je s <http://creativecommons.org/>.

# Sadržaj

- općenito o mrežnom sloju
- problemi protokola IPv4
- problemi protokola IPv6
- napadi uskraćivanja usluge
- ostvarivanje virtualnih privatnih mreža

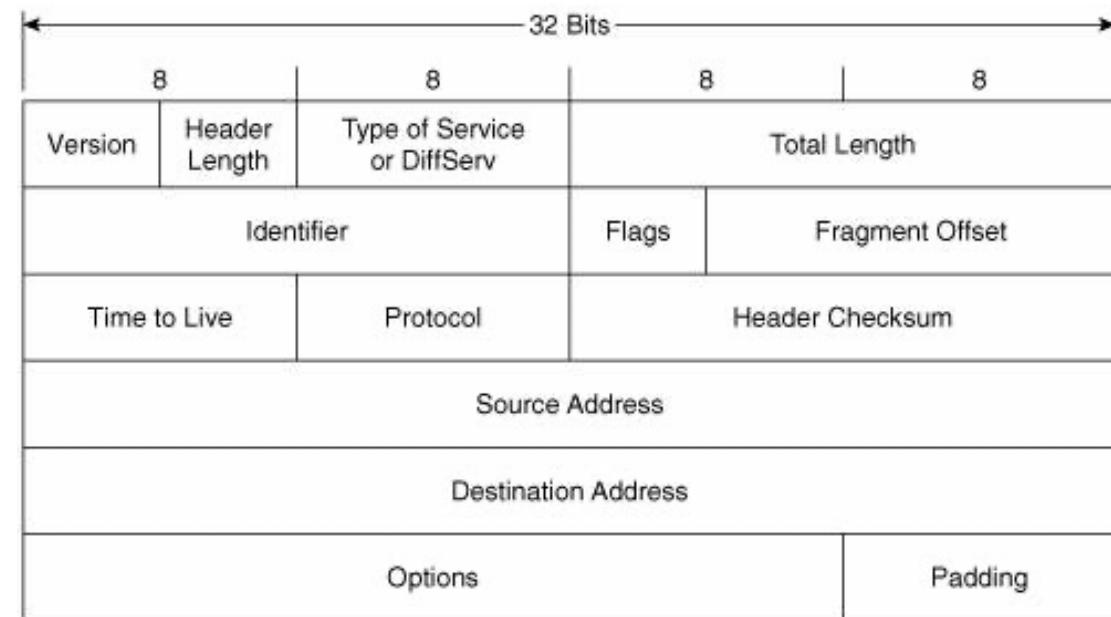
# Općenito o mrežnom sloju

- zadaća: omogućiti komunikaciju **bilo koja dva čvora u mreži**
- danas isključivo protokoli IPv4 i IPv6
  - upravljački protokoli ICMPv4 i ICMPv6
- ključna komponenta: usmjernik (engl. router)
  - osnovna zadaća: **prosljeđivanje paketa**
- ključna **sigurnosna** komponenta:  
sigurnosna stijena (vatrozid, engl. **Firewall**)
- aplikacijska sigurnost usmjernika i protokola usmjeravanja u posebnim predavanjima.



# Izvor ranjivosti protokola IPv4

- temeljna karakteristika: nespojna veza
  - jedinica podataka: datagrami/paketi
    - međusobno nezavisni
- laka izmjena pojedinih polja paketa
  - najčešće: lažiranje izvorišnih IP adresa, ne koriste se za usmjeravanje!
    - izrazito velik sigurnosni problem
- čitljivost podataka koji se prenose
  - nije ugrađena nikakva zaštita!

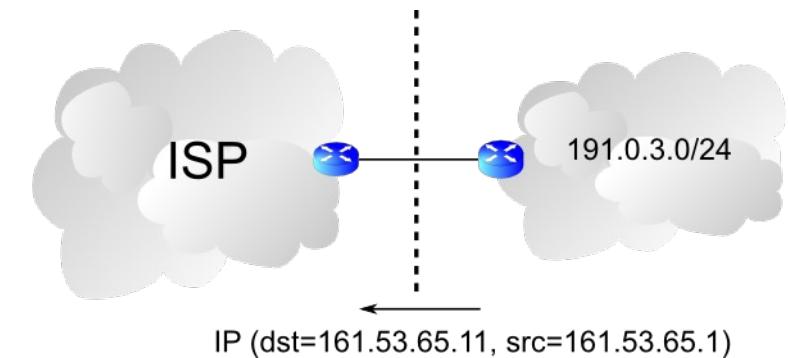


# IP zavaravanje (engl. IP spoofing)

- Slanje IP datagrama s lažnom adresom pošiljatelja
  - Najčešće se zloupotrebljava u (D)DoS napadima
- Slanje IP datagrama s lažnom adresom pošiljatelja koju primatelj smatra sigurnom
  - Zaštita:
    - Filtriranje neispravnih izvorišnih adresa
    - Zabранa korištenje IP adrese za autorizaciju i zabrana nekih servisa (onemogućavanje svih r\* naredbi: rlogin, rcp, rsh)
    - Šifriranje cijelog mrežnog prometa
- „State of IP Spoofing“ (<https://spoofercaida.org/summary.php>)

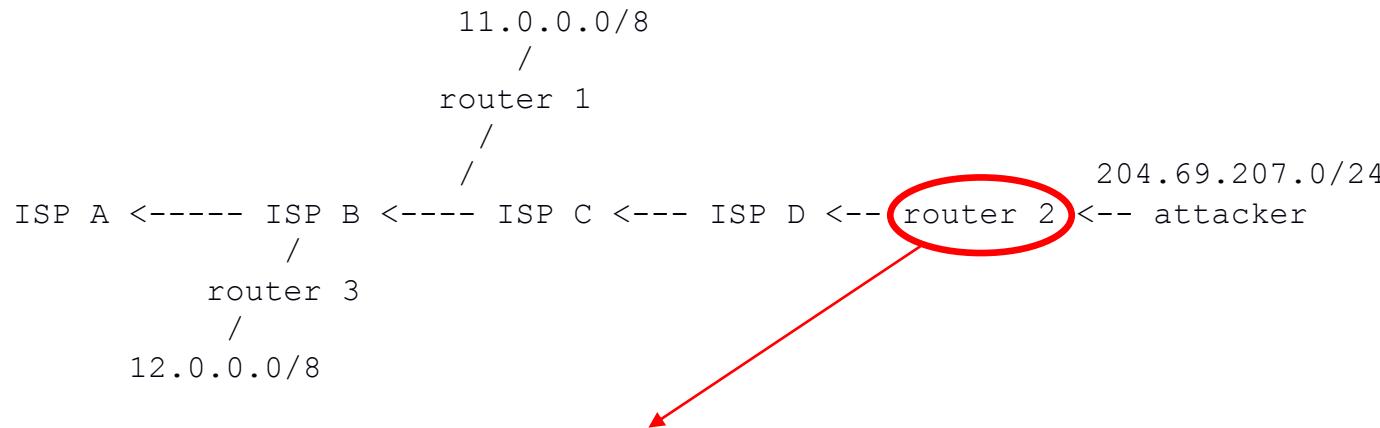
# Filtriranje neispravnih izvorišnih adresa

- Problem paketa s neispravnim izvorišnim adresama bi se djelomično riješio ispravnim podešavanjem usmjernika (RFC 2827)



- Usmjernici bi trebali filtrirati neispravne adrese
  - Međutim, to dosta često nije napravljeno
  - Posljedica: (D)DoS napadi
- Privatne IP adrese također moraju biti filtrirane
  - 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, nealocirane IP adrese

## RFC 2827 – “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”



- ISP D na ruteru 2 filtrira dolazne pakete od napadača (*attacker*):

IF packet's source address from within 204.69.207.0/24

THEN forward as appropriate

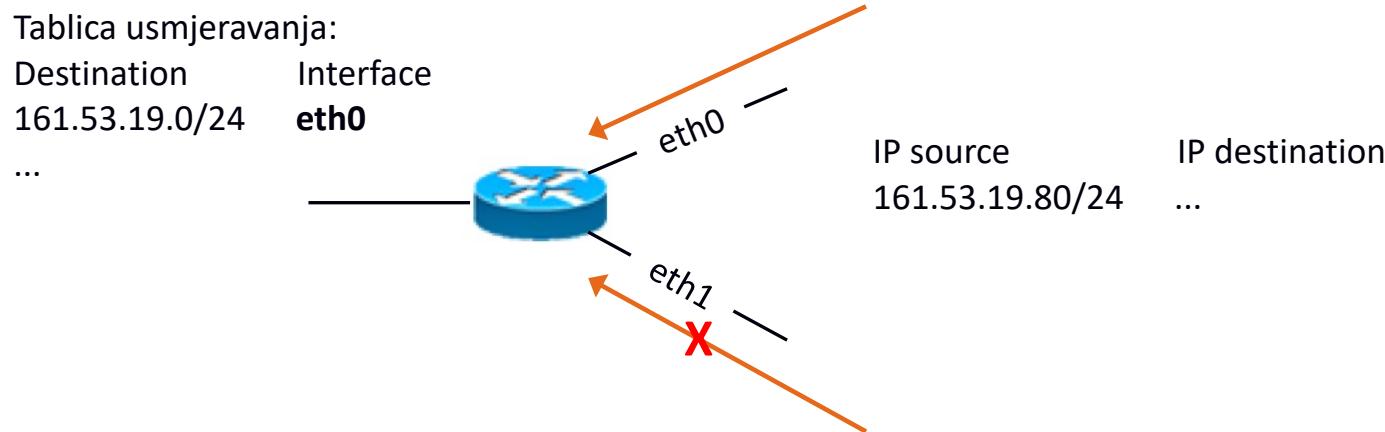
IF packet's source address is anything else

THEN deny packet

- a napadač (“*attacker*”), za svoju zaštitu, može filtrirati sve dolazne pakete iz Interneta s izvořišnom adresom 204.69.207.0/24

# Dobre prakse za „anti-spoofing”

- uRPF (unicast Reverse-Path Forwarding)
  - filtriranje na ulazu u mrežu
  - IP datagram se propušta ako za njegovu izvorišnu adresu postoji zapis u tablici usmjeravanja i paket dolazi po istom sučelju po kojem bi bio poslan na to odredište
  - malo komplikiranije kod asimetričnog usmjeravanja (veza na više ISP)



# Dobre prakse za „anti-spoofing”

- Radius/Diameter + dinamičke pristupne liste (access list)
  - prilikom autentifikacije korisnika osvježi se i pristupna lista
- „Source Address Validation Improvements“ (SAVI)
  - praćenje (*snooping*) poruka DHCPv4 i DHCPv6 (u Cisco terminologiji: „source guard“ i „prefix guard“)

# “Nonroutable” mrežne adrese

- 0.0.0.0/8
  - na primjer DHCP “broadcast request”
- 127.0.0.0/8
  - na primjer localhost 127.0.0.1
- 169.254.0.0/16
  - DHCP “autoconfigure”
- 192.0.2.0/24
  - "TEST-NET," alocirano za primjere i dokumentaciju
- 198.18.0.0/15
  - RFC 2544, testiranje performansi
- 224.0.0.0/4
  - multicast adrese, filtrirati ako se ne koriste
- 240.0.0.0/4
  - stara klasa E

# IP fragmentacija

- Fragmentacija je obavezan dio IP protokola; kad je potrebno datagram podijeliti na manje dijelove prije učahurivanja u okvir podatkovne veze  
**(duljina IP datagrama > MTU)**
  - Moguće na izvorišnom računalu i na svakom usmjeritelju na putu do odredišta
  - Svaki fragment se dostavlja nezavisno
  - Može zavarati neke vatrozide i sustave za detekciju uljeza

# IP fragmentacija

- Datagram se sastavlja na krajnjem odredištu
  - svaki fragment se usmjerava nezavisno
- Svi fragmenti imaju isti identifikacijski broj (IP ID)
- Pomak (*fragment offset*) određuje smještaj fragmenta u sastavljenom datagramu
- Zastavica “*more fragments*” postavljena je u svim fragmentima osim u zadnjem

# IP fragmentacija - primjeri napada

- „Ping of Death” (1996.)
  - DoS (“Denial of Service”) napad koji prekoračuje maksimalnu veličinu IP datagrama
  - kreira se i šalje fragmentirani IP datagram ukupne duljine veće od 65535 okteta
  - teoretski bilo koji IP paket, ali obično baš “ICMP echo request”
  - “*Fragment Offset*” je takav da je ukupna veličina zapakiranog datagrama veća od maksimalno dozvoljene veličine: → *buffer overflow, kernel panic*
- „Teardrop” (Linux kernel < 2.0.32)
  - napadač šalje dva fragmenta koji se djelomično prekrivaju
  - “crash” kernela nakon sastavljanja fragmenata.
- Ima i novijih:
  - search “IP fragmentation”: [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)

# IP fragmentacija - primjeri napada

- "*TCP overwrite*"
  - varijacija napada "teardrop"
  - nije napad tipa DoS već se pokušava prevariti vatrozid
  - IP datagram se fragmentira, TCP zaglavje sadrži dozvoljeni port, na primjer 80, pa ga vatrozid propušta
  - neki sljedeći fragment ima „pomak“ postavljen na 1 što znači da će port biti prepisan (npr. novi port će biti 23), sastavljeni paket preusmjerava se na novi port
  - vatrozid treba provjeravati minimalni pomak fragmenta!

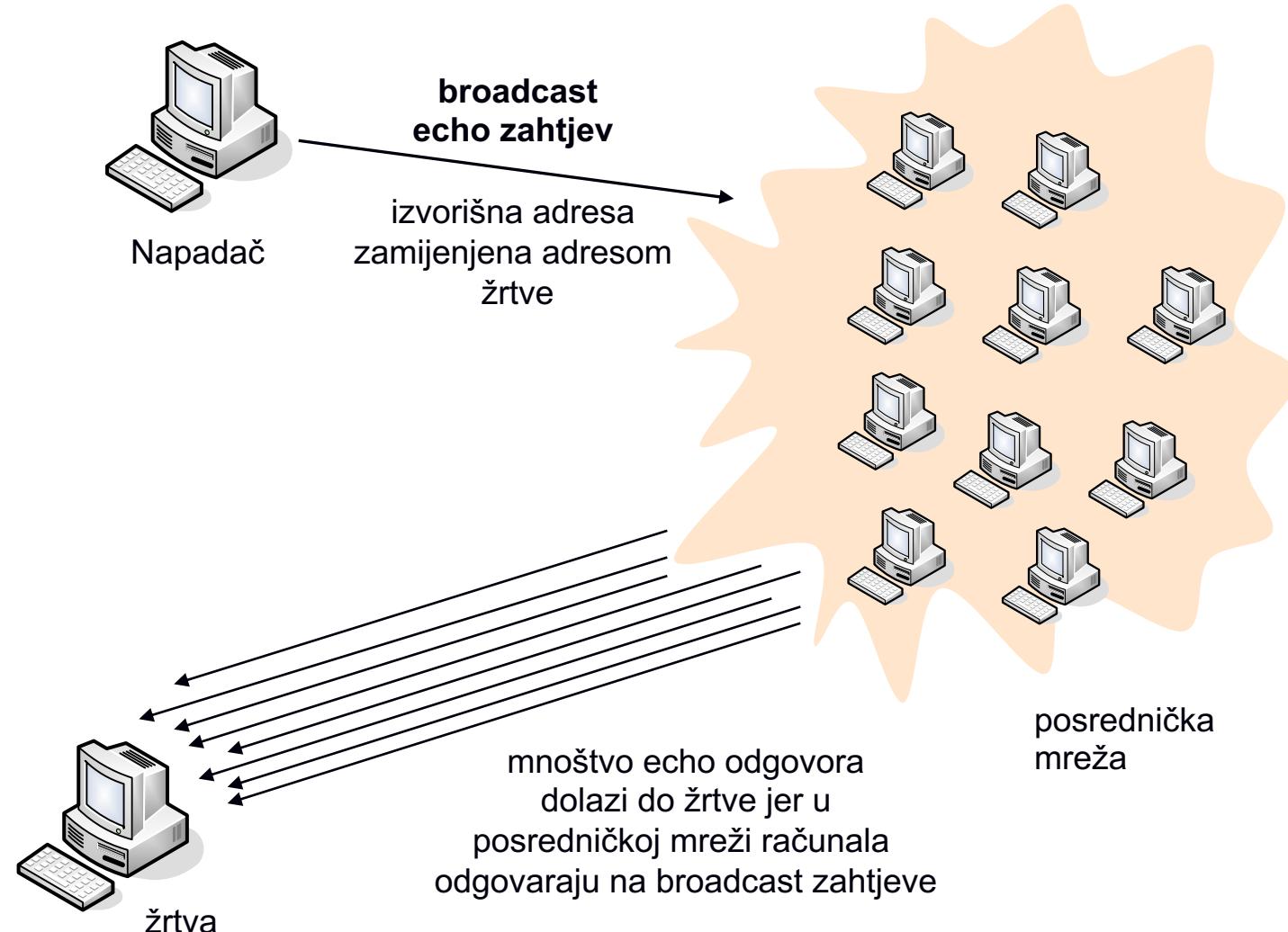
# Ranjivosti i zloupotrebe protokola ICMP

- U pravilu se radi o DoS napadima
- Iskorištavanje tipa „ICMP redirect” za zlonamjerno preusmjeravanja prometa
- Uskraćivanje usluge slanjem lažiranih ICMP poruka o nedostižnom odredištu
- Implementacija prikrivenih kanala (engl. covert channel) korištenjem ICMP poruka
- Enumeracija računala na mreži

# Ranjivosti i zloupotrebe protokola ICMP

- napad “smurf”

- započinje slanjem echo zahtjeva na sveodredišnu (“broadcast”) adresu posredničke mreže s lažiranom izvorišnom adresom jednakom adresi ciljne mreže (žrtve)
- računala u posredničkoj mreži odgovaraju slanjem echo odziva
- odgovori idu na adresu žrtve
- posrednička mreža i ciljna mreža zagušene prometom
- napad se pojačava slanjem zahtjeva na različite posredničke mreže



# Protokol DHCP

- Služi za automatsku dodjelu adresa i mrežnih parametara
  - Klijent šalje svima na mreži poruku DHCPDISCOVER
    - Klijent u tom trenutku ne zna adresu
  - Poslužitelji odgovaraju klijentu s porukom DHCPOFFER
  - Klijent odabire poslužitelj i šalje svima DHCPREQUEST
  - Poslužitelj odgovara s DHCPACK
- Fiksiranje adresa na temelju MAC adrese radi kontrole pristupa
  - Moguće i na temelju identifikatora

# Problemi protokola DHCP

- Nema nikakve zaštite poruka
  - Bilo tko može slati i primati DHCP poruke
- Lažni DHCP poslužitelji na mreži
  - Napadi uskraćivanja usluga
  - Preusmjeravanje prometa
- Bilo koji klijent može zatražiti parametre
  - Lako se zaobilazi MAC/ID zaštita
  - Moguće iscrpljivanje svih raspoloživih adresa („DHCP Starvation attack“)

# Protokol IPv6

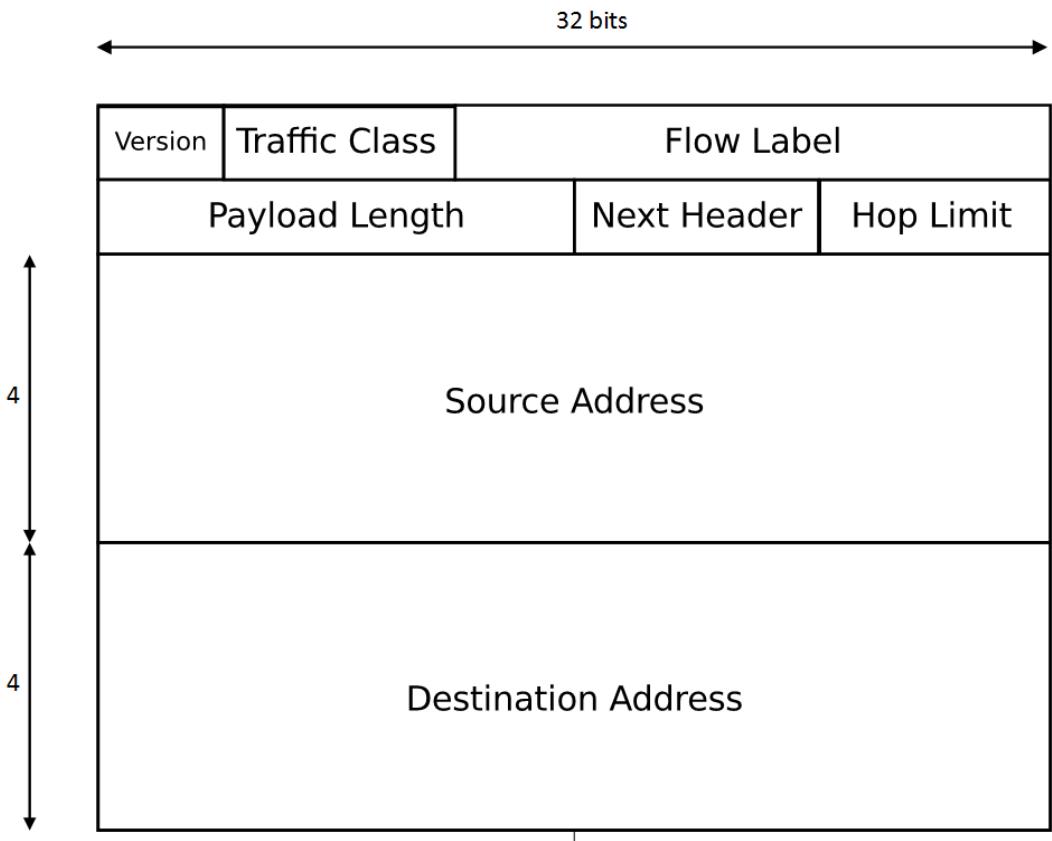
- Zašto uopće spominjati sigurnost protokola IPv6?
  - Na razini RIR-ova IPv4 adrese su iscrpljene te je neminovno uvođenje IPv6
  - Značajni napori da se popularizira i uvede IPv6
- Dosta operacijskih sustava već ima omogućen IPv6
  - Windows OS počevši sa Windows Vista u podrazumijevanoj konfiguraciji ima omogućen IPv6
  - Linux / BSD / macOS već dugo vremena imaju omogućen IPv6 u standardnoj konfiguraciji
- Koliko ljudi je toga svjesno?

# Cilj razmatranja protokola IPv6

- Upozoriti na činjenicu kako je IPv6 drugačiji od IPv4
  - IPv6 nije radikalno drugačiji, ali je dovoljno da ima svojih specifičnosti
- Nedostatak operativnog iskustava
- Upoznati se s ranjivostima
  - Specifičnim za protokol IPv6
  - Koje ranjivosti su zajedničke
  - Kojih ranjivosti više nema u odnosu na protokol IPv4

# Promjene u protokolu IPv6 u odnosu na IPv4

- Osnovne izmjene u protokolu IPv6
  - Adrese su 128 bita
  - Pojednostavljeni zaglavljci
  - Fragmentacija se više ne provodi u mrežnom sloju
  - ARP se više ne koristi
  - Automatsko podešavanje mrežnih parametara
- Zaglavljci protokola IPv6 i dalje nema zaštite!



# IPv6 adrese

- Adrese su 128 bitne
  - Pišu se u 8 grupa po 16 bita, svaka grupa 4 heksadecimalne znamenke
- Primjeri
  - 1234:5678:9abc:def0:1234:5678:9abc:def0
  - 1234:5678:0000:0000:1234:0000:0000:def0
  - 1234:5678:0:0:1234:0:0:def0, 1234:5678::1234:5678:0:def0,
  - 1234:5678:0:0:1234::def0
- Klase adresa
  - lokalne (link local), globalne, višeodredišne (multicast)
  - „Anycast” podskup globalnih adresa

# Ranjivosti kojih više nema u IPv6

- Odnosno, one koje su umanjene.
- Skeniranje IPv6 mreža je otežano, ali
  - Postoje specifične adrese:
    - Svi čvorovi: FF01::1, FF02::1
    - Svi usmjernici: FF01::2, FF02::2
    - All DHCP agents: FF02::1:2
  - Korisnici će vjerojatno dodjeljivati lako pamtljive adrese uređajima
- Ne koriste se više broadcast adrese
- Onemogućena je fragmentacija u usmjernicima

# Ranjivosti zajedničke protokolima IPv4 i IPv6

- Skeniranje jedne adrese je i dalje moguće
- Razrješavanje IP adresa u MAC adresu
  - Ne koristi se više ARP već ICMPv6, ali sve je ostalo isto
- Protokoli ICMPv4 i ICMPv6 i dalje ranjivi
- Protokol DHCP se i dalje koristi u obje mreže
- Protokol IPsec se koristi za zaštitu oba protokola
  - Krivo se ponekad kaže kako je IPv6 sigurniji od IPv4
  - Jedina razlika je što u normama piše da se mora implementirati IPsec ako implementacija želi biti uskladiva s IPv6 normom
  - Ali, implementacije za IPv4 i IPv6 jednako podržavaju IPsec

# Ranjivosti specifične za protokol IPv6 (1)

- Samostalno podešavanje IPv6 adrese
  - Obavlja se na temelju MAC adrese.
  - Problem s privatnošću.
    - Mogućnost slučajno generiranih IPv6 adresa, ali one su također problematične!
- Problem velikog adresnog prostora
  - Teško je kontrolirati tko koristi koju adresu.
  - Problem za sigurnosne stijene jer potencijalno trebaju čuvati puno podataka.
- Višeodredišne adrese
  - Lako propitivanje za pojedinim uređajima na lokalnoj mreži

# Ranjivosti specifične za protokol IPv6 (2)

- Zloupotreba mehanizma DAD (Duplicate address detection) radi uskraćivanja usluge
- Objava usmjerničkih podataka
  - Napadač lakše dolazi do informacija potrebnih za spajanje
  - Može slati lažirane objave usmjerničkih podataka
- Nedostatak operativnog iskustva
- Automatsko tuneliranje
  - Uvedeno radi tranzicije s IPv4 na IPv6
- Sigurnosni uređaji još nisu dovoljno sazreli

# Protokol ICMPv6

- Vrlo značajan za ispravan rad protokola IPv6
  - Daleko značajniji no što je to bio ICMPv4 za IPv4
- Posljedično, nije moguće filtrirati sav ICMPv6 promet
  - Mreža neće raditi
  - Razrješavanje IPv6 u MAC adresu, autokonfiguracija, ...

# Poboljšanje sigurnosti na mrežnom sloju

- Protokol IP ne nudi nikakvu zaštitu
  - Može se lažirati, sadržaj lako čitljiv
  - Kako sigurno povezivati lokalne mreže i udaljene korisnike?
- Opcije na mrežnom sloju
  - Kriptiranje i zaštita integriteta
    - Virtualne privatne mreže (engl. Virtual Private Networks, VPNs)
- Za potpunu zaštitu preporučljivo je koristiti i (komplementarna) rješenja na višim slojevima
  - TLS/HTTPS/SSH ili neka druga metoda kriptiranja i autentikacije
  - Moguće je navedene protokole koristiti i bez zaštite u mrežnom sloju!

# Internet / Intranet / Extranet

- Internet - javna mreža
- Intranet
  - privatna mreža (unutar kompanije, institucije)
  - tehnologija ista kao i kod Interneta
  - obično se koriste privatne IP adrese, no mogu se koristiti i javne
    - pod uvjetom da IP paketi nikada ne budu poslani na Internet
  - različite lokacije povezuju se preko WAN ili VPN veza
- Extranet
  - proširenje pojma Intranet
  - korisnici i izvan kompanije/institucije
  - dobavljači, proizvođači, partneri, korisnici
  - sigurnost i privatnost

# Udaljeni pristup Intranetu

zahtjevi:

- privatnost – integritet podataka
  - korištenje enkripcijskih mehanizama na strani klijenta i servera:
  - protokol za sigurnu razmjenu kriptografskih ključeva (na primjer IKE, TSL)
  - algoritmi za enkripciju i
  - metode provjere integriteta podataka
- umrežavanje
  - podrška za korištenje IP protokola i mrežne infrastrukture:
  - mogućnost rada iza vatrozida, uz prisutne NAT uređaje i proxy poslužitelje
  - korištenje dinamički dodijeljenih IP adresa
- upravljivost
- kontrola pristupa

# Udaljeni pristup Intranetu

(zahtjevi)

- upravljivost
  - korištenje različitih načina autentifikacije (na primjer korištenje digitalnih certifikata X.509, standardnih lozinki operacijskog sustava i slično)
  - korištenje direktorija (LDAP, RADIUS, Active Directory) za pohranjivanje i održavanje informacija o korisnicima
- kontrola pristupa
  - mogućnost administriranja nivoa pristupa:
    - enkripcijske tehnike mogu osigurati privatnost i integritet podataka ali one ne pridjeljuju prava pristupa korisnicima
    - ako korisnik može uspostaviti VPN tunel (bez obzira na korištenu tehnologiju) to ne znači da smije imati pristup svim resursima mreže

# “Sigurni” udaljeni pristup intranetu

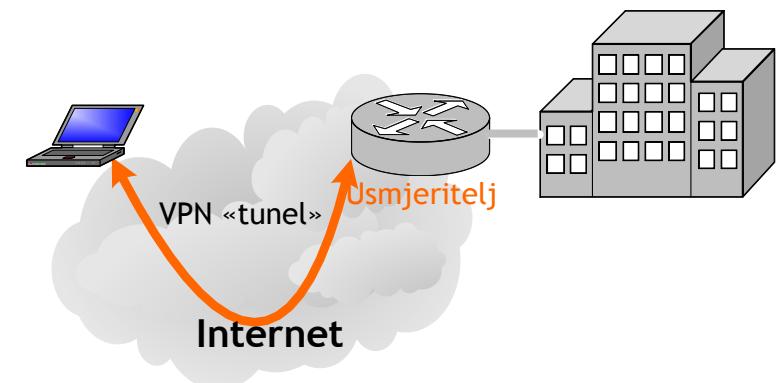
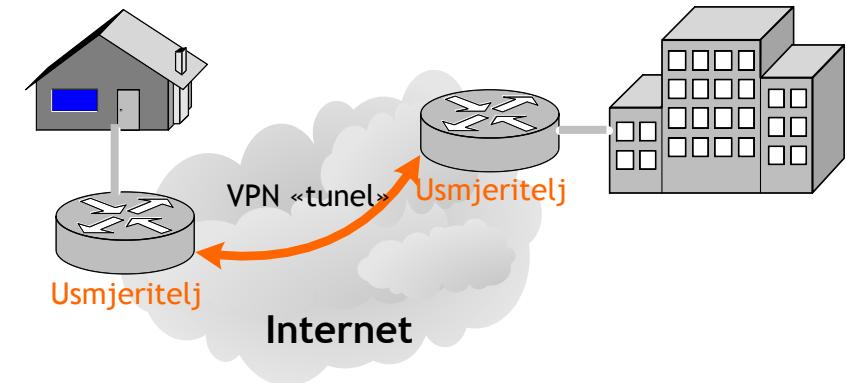
- Virtualne privatne mreže, VPN, „Virtual Private Networks”
  - ista (sigurnosna) politika i performanse kao i privatne mreže realizirane preko infrastrukture WAN
  - sigurni VPN (Secure VPN):
    - autentifikacija korisnika/računala, tajnost i integritet podataka

# Virtualne privatne mreže

- Virtual Private Networks (VPN)
  - Pojam koji označava stvaranje privatnih mreža nad javnom infrastrukturom Interneta
  - Zamjena za nekadašnje iznajmljivanje linkova, modeme, i slično.
  - Nije specifičnost mrežnog sloja, ali je nužno prenositi IP pakete
- Rješenja za ostvarenje virtualnih privatnih mreža
  - PPTP – ne koristiti!
  - OpenVPN
  - WireGuard
  - IPsec (verzije 2 i 3) – standardni dio IPv6 (i IPv4), kompleksna konfiguracija
    - IPsec+L2TP
  - „Clientless VPN” - TLS

# Vrste VPN

- od točke do točke (*Site-to-site*)
  - između dva mrežna entiteta (na primjer usmjeritelja)
  - privatne i zaštićene mreže iza oba entiteta
- udaljeni pristup (*Remote Access*)
  - između uređaja i usmjeritelja
  - na udaljenoj lokaciji se ne nalazi zaštićena mreža



# Osnove arhitekture IPsec (1)

- Rješenje na mrežnom sloju
- Služi za
  - povezivanje dviju ili više mreža (VPN)
  - povezivanje osobnih računala na korporativnu mrežu (engl. road-warrior)
  - povezivanje dva računala međusobno
- Može raditi u tunelskom i prijenosnom načinu rada
- Autentifikacija putem certifikata, dijeljene tajne ili EAP-a
- Najčešće upotrebljavana je verzija 2 a najnovija je verzija 3

# Osnove arhitekture IPsec (2)

- Protokol definira ponašanje krajnjih točaka i protokole za razmjenu upravljačkih informacija i podataka
- Ponašanje krajnjih točaka definirano bazama SPD i SAD
- Osnovni protokoli
  - IKE: Uspostava ključeva, implementira se u korisničkom načinu rada u vidu aplikacije
  - ESP: Encapsulating Security Payload  
Zaštita tajnost, integriteta i autentičnosti, impl. u jezgri operacijskog sustava
  - AH: Authentication Header  
Zaštita integriteta i autentičnosti, impl. u jezgri operacijskog sustava

# IPsec

IP zaglavlje

IP podaci (*payload*)

GRE (Generic Routing Encapsulation), protokol: 47

IP zaglavlje

GRE

IP zaglavlje

IP podaci (*payload*)

## IPsec transportni način

IP zaglavlje

ESP zaglavlje

IP podaci (*payload*)

ESP trailer

Auth

šifrirano (encrypted)

ovjereno (authenticated)

## IPsec tunelirani način

IP zaglavlje

ESP zaglavlje

IP zaglavlje

IP podaci (*payload*)

ESP trailer

Auth

šifrirano (encrypted)

ovjereno (authenticated)

# IPsec

- „An Illustrated Guide to IPsec”
  - <http://www.unixwiz.net/techtips/iguide-ipsec.html>

# Baze SPD i SAD (1)

- **SPD** (Security Policy Database) definira što se treba zaštititi
  - Način zaštite (tunel ili prijenosni način)
  - Sadrži selektore prometa
    - Selektor se sastoji od IP adrese/mreže, protokole, pristupe; za svaku stranu veze posebno
  - Navodi što treba učiniti s paketom koji odgovara
    - Blokirati, propustiti ili zaštititi
- **SAD** (Security Association Database) definira kako treba štititi
  - Sadrži odabrane kriptografske algoritme i ključeve

# Baze SPD i SAD (2)

- Primjer ispisa SPD baze na Linux OS-u

```
172.16.228.0/24[any] 192.168.173.0/24[any] any
  out prio def ipsec
  esp/tunnel/161.53.65.225-161.53.65.11/require
  created: Nov 22 15:52:52 2010 lastused:
  lifetime: 0(s) validtime: 0(s)
  spid=17 seq=1 pid=16163
  refcnt=1
```

```
192.168.173.0/24[any] 172.16.228.0/24[any] any
  in prio def ipsec
  esp/tunnel/161.53.65.11-161.53.65.225/require
  created: Nov 22 15:52:52 2010 lastused:
  lifetime: 0(s) validtime: 0(s)
  spid=8 seq=0 pid=16163
  refcnt=1
```

# Baze SPD i SAD (3)

- Primjer ispisa SAD baze na Linux OS-u

```
161.53.65.225 161.53.65.11
esp mode=tunnel spi=15702(0x00003d56) reqid=0(0x00000000)
E: 3des-cbc 31323334 35363738 39303132 31323334 35363738 39303132
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Nov 22 15:52:52 2010           current: Nov 22 15:56:41 2010
diff: 229(s)   hard: 0(s)   soft: 0(s)
last:          hard: 0(s)   soft: 0(s)
current: 0(bytes)    hard: 0(bytes) soft: 0(bytes)
allocated: 0   hard: 0       soft: 0
sadb_seq=1 pid=16330 refcnt=0
```

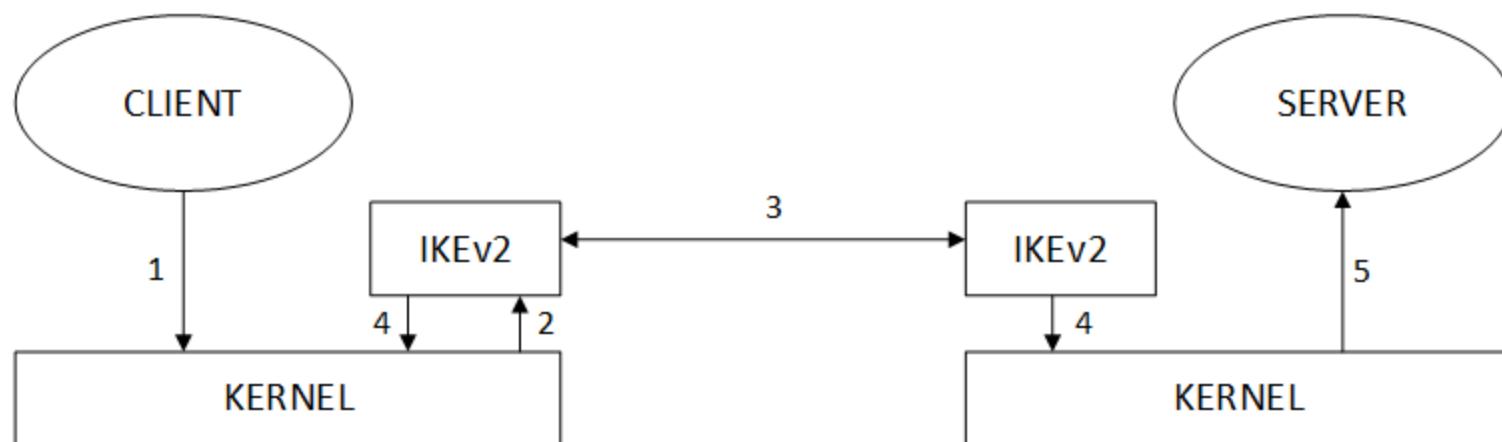
```
161.53.65.11 161.53.65.225
esp mode=tunnel spi=15701(0x00003d55) reqid=0(0x00000000)
E: 3des-cbc 31323334 35363738 39303132 31323334 35363738 39303132
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Nov 22 15:52:52 2010           current: Nov 22 15:56:41 2010
diff: 229(s)   hard: 0(s)   soft: 0(s)
last:          hard: 0(s)   soft: 0(s)
current: 0(bytes)    hard: 0(bytes) soft: 0(bytes)
allocated: 0   hard: 0       soft: 0
sadb_seq=0 pid=16330 refcnt=0
```

# Protokol IKEv1 i IKEv2

- Skraćenica od Internet Key Exchange
- Zadaće protokola su
  - Autentifikacija partnera
  - Dogovor oko sigurnosnih asocijacija (engl. security associations, SA)
  - Periodička razmjena ključeva
- Razlike IKEv2 u odnosu na IKEv1
  - IKEv2 pojednostavljen u odnosu na IKEv1
  - Potrebno je manje razmjena paketa kako bi se uspostavila prva sigurnosna asocijacija
  - Uklonjena i jedna ranjivost u posebnom načinu rada

# Primjer rada protokola IKE i ESP/AH

- Neka aplikacija na lijevom računalu želi pristupiti aplikaciji na desnom računalu
  - Prikazan je slijed komunikacije pod uvjetom da te dvije aplikacije nisu prethodno komunicirale



# Prednosti IPsec arhitekture

- IPsec je izведен ispod transportnog sloja
  - za potpunu funkcionalnost (ipak) potrebna prilagodba aplikacija i API-ja
  - može se izvesti u krajnjem korisnikovom računalu ili u mrežnom uređaju: vatrozidu (firewall) ili usmjeritelju
- ako je IPsec zaključen u vatrozidu ili usmjeritelju, uređaj osigurava granicu prema ostatku mreže
  - lokalni promet se ne opterećuje sigurnosnim mehanizmima
  - osiguran je siguran pristup s autentificiranog mrežnog sučelja iz vanjske mreže
  - omogućeno je sigurno povezivanje dislociranih mreža, npr. na raznim lokacijama iste tvrtke, preko nesigurnog javnog Interneta (primjena: virtualna privatna mreža)
- kod usmjeravanja, IPsec osigurava identitet usmjeritelja

# Sigurnosne usluge IPsec arhitekture

- kontrola pristupa
  - "sigurnosna granica" između zaštićenih i nezaštićenih sučelja
- cjelovitost na razini datagrama
  - cjelovitost nekonekcijskog toka, npr. UDP prometa
- vjerodostojnost izvora datagrama
- zaštita protiv napada ponovnim slanjem snimljenog prometa
  - vrsta napada pri kojem se ponovnim slanjem snimljenih paketa (npr. prilikom prijave na sustav) pokušava neovlašteno ostvariti pristup ili neka radnja na sustavu
- povjerljivost (šifriranje prometa)
- ograničena povjerljivost prometnog toka
  - izvođačna i odredišna IP adresa su vidljive, ali se ne vidi izvor i odredište na transportnom sloju (port)
- nedostaci:
  - ne autentificira se korisnik, već računalo
  - nema sigurnosti ako sam sistem nije siguran ili ako je već kompromitiran



SVEUČILIŠTE U ZAGREBU



Diplomski studij

Ak. godina 2022./2023.

# Sigurnost komunikacija

Sigurnost transportnog sloja



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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.

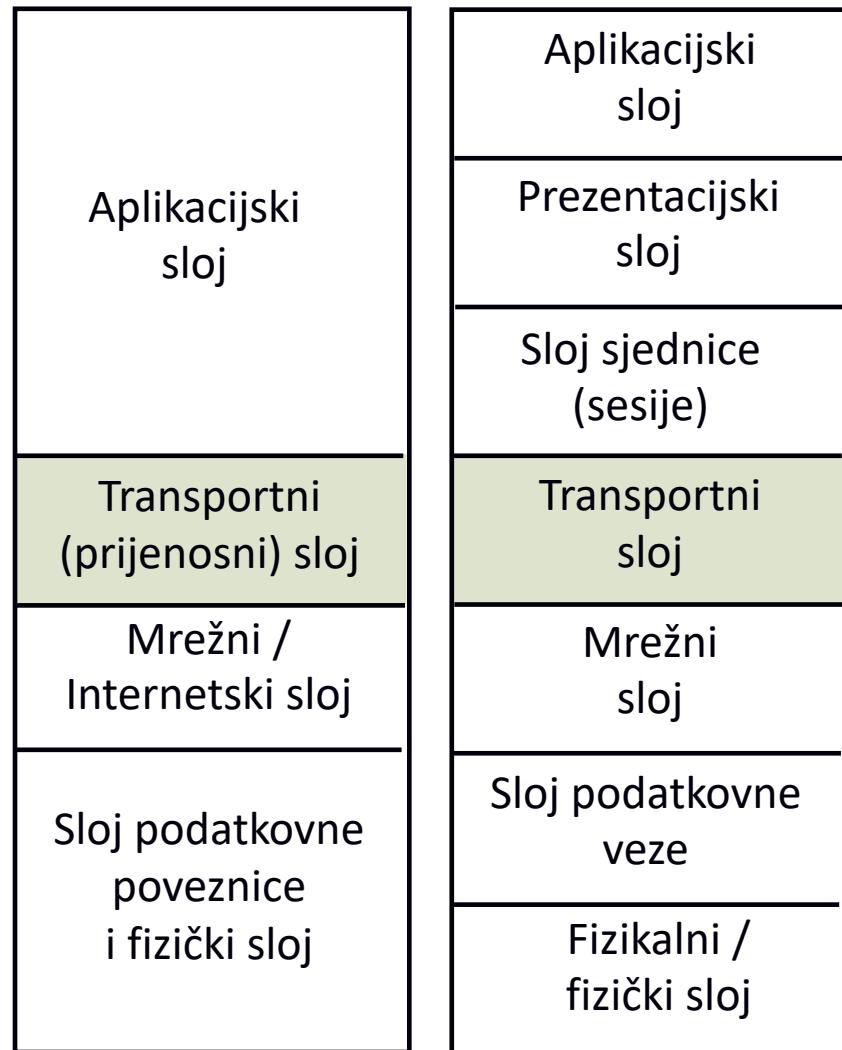
Tekst licencije preuzet je s <http://creativecommons.org/>.

# Sadržaj

- općenito o prijenosnom sloju
- temelji protokola UDP
- napadi na protokol UDP
- temelji protokola TCP
- napadi na protokol TCP
- sigurnosna rješenja

# Općenito o transportnom sloju

- omogućava komunikaciju s kraja-na-kraj
- najčešći protokoli na Internetu:
  - TCP (~70%) i UDP (~30%)
  - postoji još SCTP, DCCP, QUIC
- protokol TCP
  - upotrebljava ga niz aplikacija (web (http/https), elektronička pošta, protokoli usmjeravanja, prijenos datoteka, udaljeni rad, ...)
- sve češća upotreba protokola UDP:
  - višemedijske aplikacije, VoIP, neki sistemski protokoli Interneta (DNS)

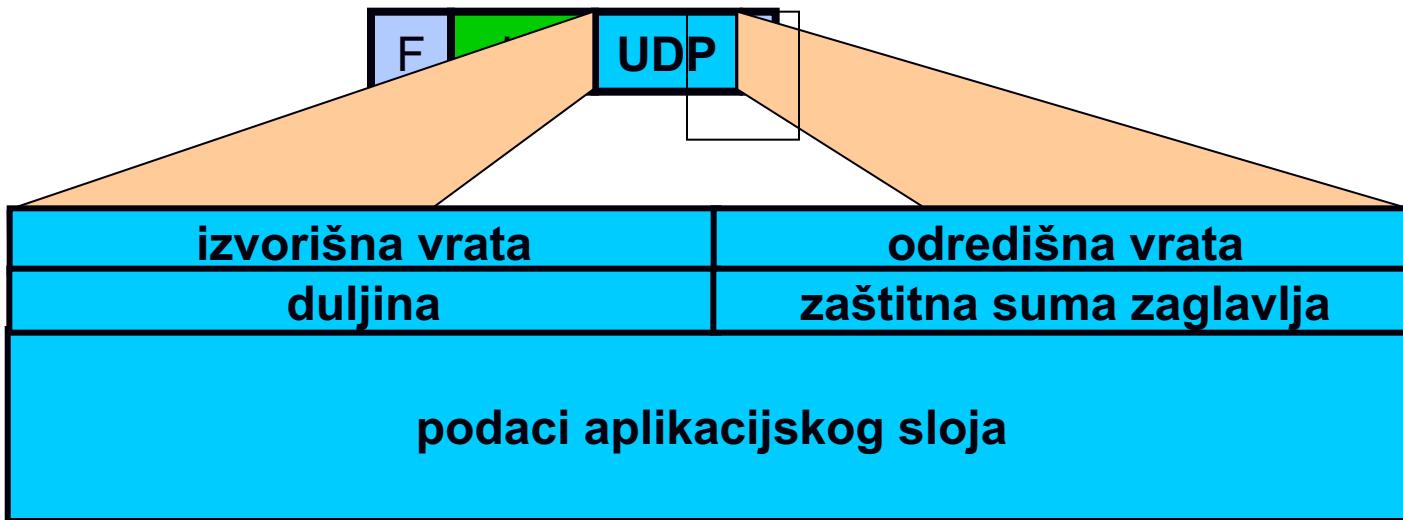


# Protokol UDP

- Nespojni transportni protokol
- Nema ugrađene mehanizme za pouzdan prijenos
- Nema kontrole toka
- Često se koristi za prijenos višemedijskih podataka (efikasniji je od TCP) i za usluge temeljene na principu zahtjev / odziv (DNS, NIS, NFS, RPC)

# Protokol UDP

- duljina UDP zaglavlja: 8 okteta



# Napadi na UDP

- UDP obмана - (*UDP spoofing*)
  - mijenjanjem izvorišne IP adrese “predstavljamo se” kao drugo računalo
  - IP adresa je jedini način identifikacije računala u protokolu UDP
  - ne šalju se potvrde
- UDP otimanje - (*UDP hijacking*)
  - napadač sluša vezu
  - odgovara na klijentov UDP zahtjev prije poslužitelja slanjem paketa s promijenjenom izvorišnim adresom
  - klijent misli da je primio paket od poslužitelja
  - nema identifikacije paketa

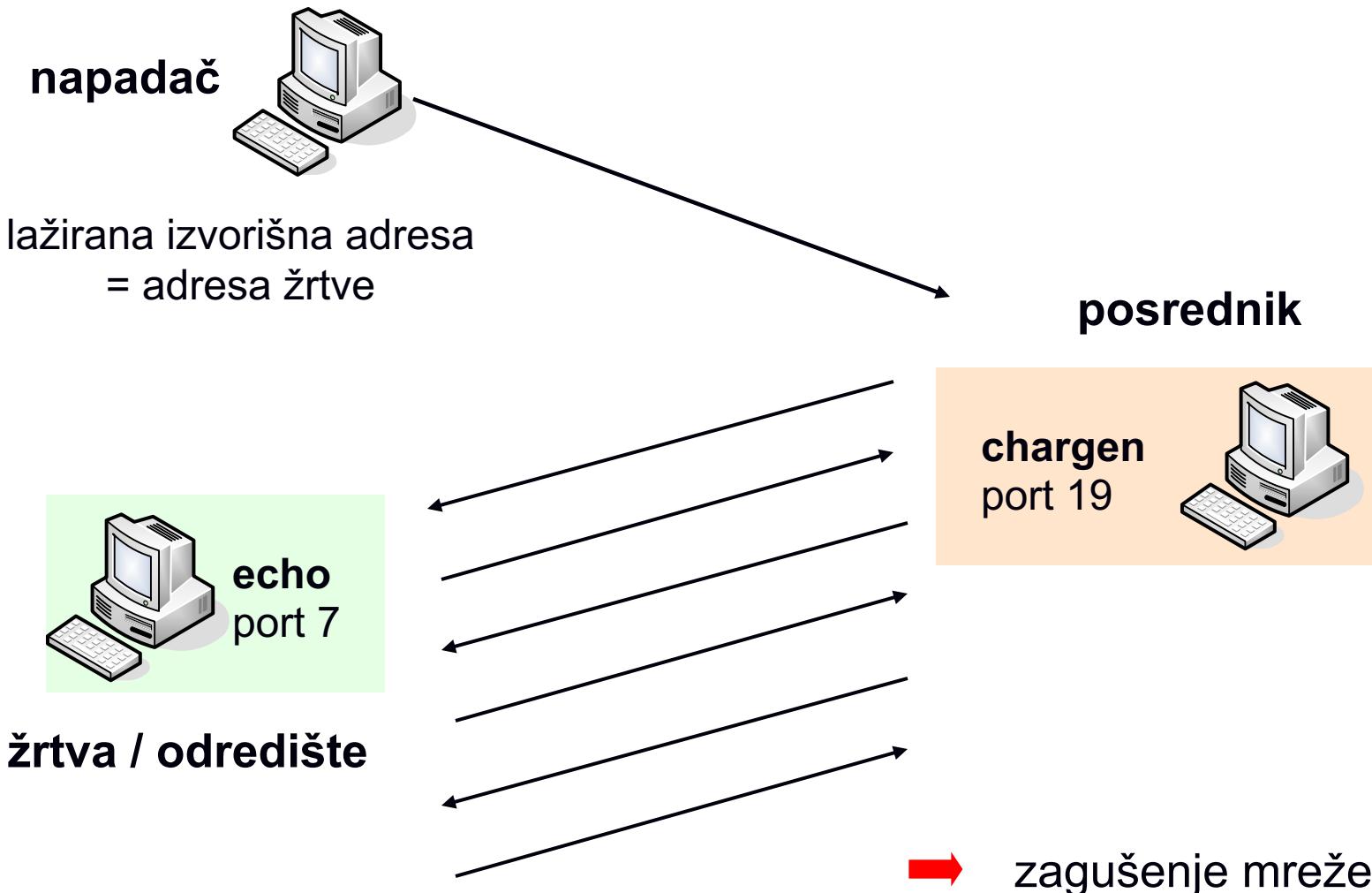
# Napadi na UDP

- UDP oluće - (*UDP storms*)
  - jedan paket je dovoljan za pokretanje napada!
  - obično se pošalje nekoliko paketa kako bi se pojačalo djelovanje
  - može se koristiti bilo koji servis koji automatski odgovara na primljeni UDP datagram: echo (7), chargen (19), daytime (13), time (37), ...
  - i usmjeritelji često podržavaju nekoliko dijagnostičkih usluga
  - petlja se izvodi dok jedno računalo ne završi (može biti potreban i reboot)

# UDP Small Services

Naziv	Port	Opis usluge
echo	7/udp	server echoes the data that the client sends
daytime	13/udp	server returns the time and date in a human readable format
chargen	19/udp	server responds with a datagram containing a string of ascii characters
time	37/udp	server returns the time as a 32-bit binary number

# UDP storm / UDP flood



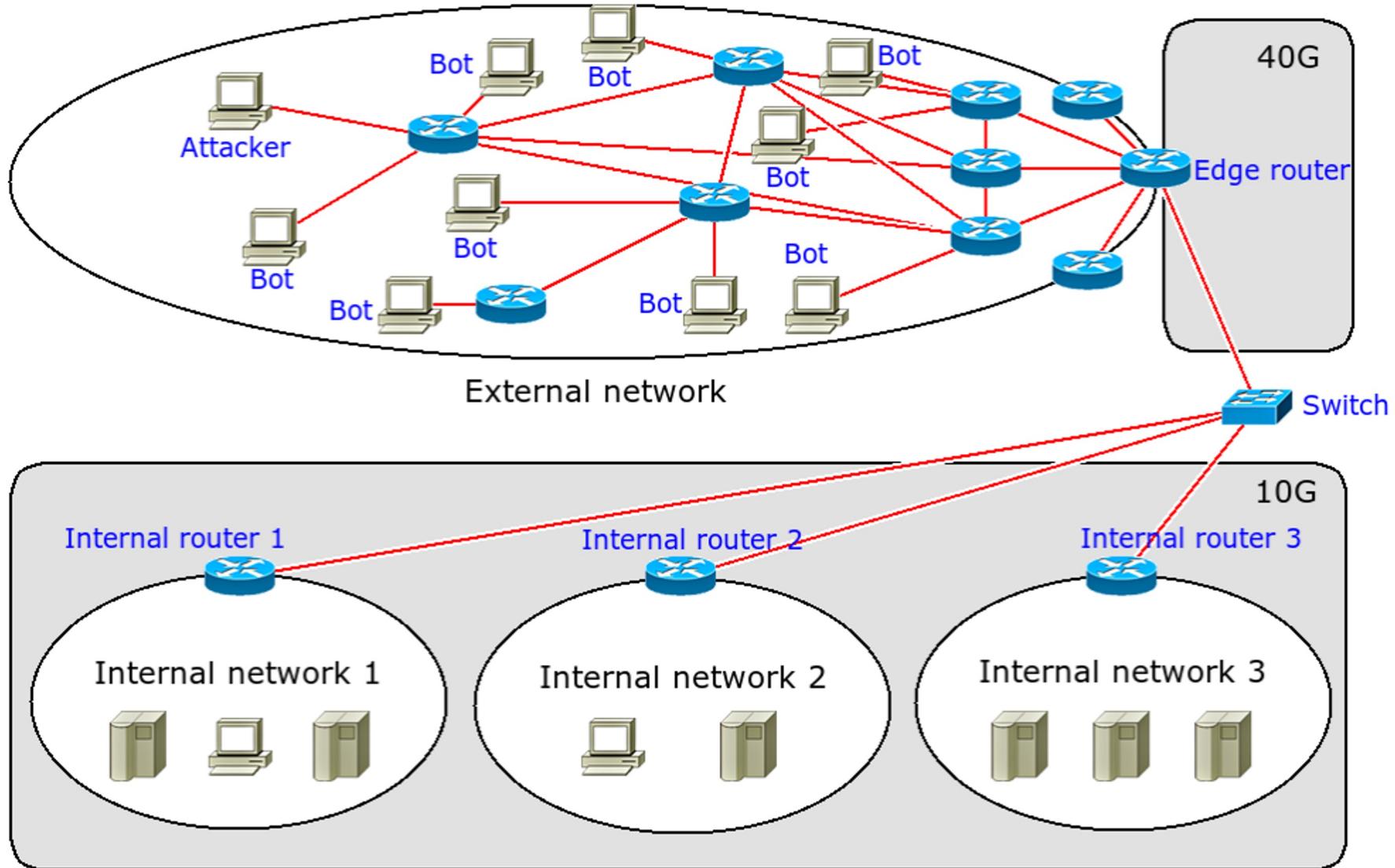
# DoS - Napadi uskraćivanja usluge

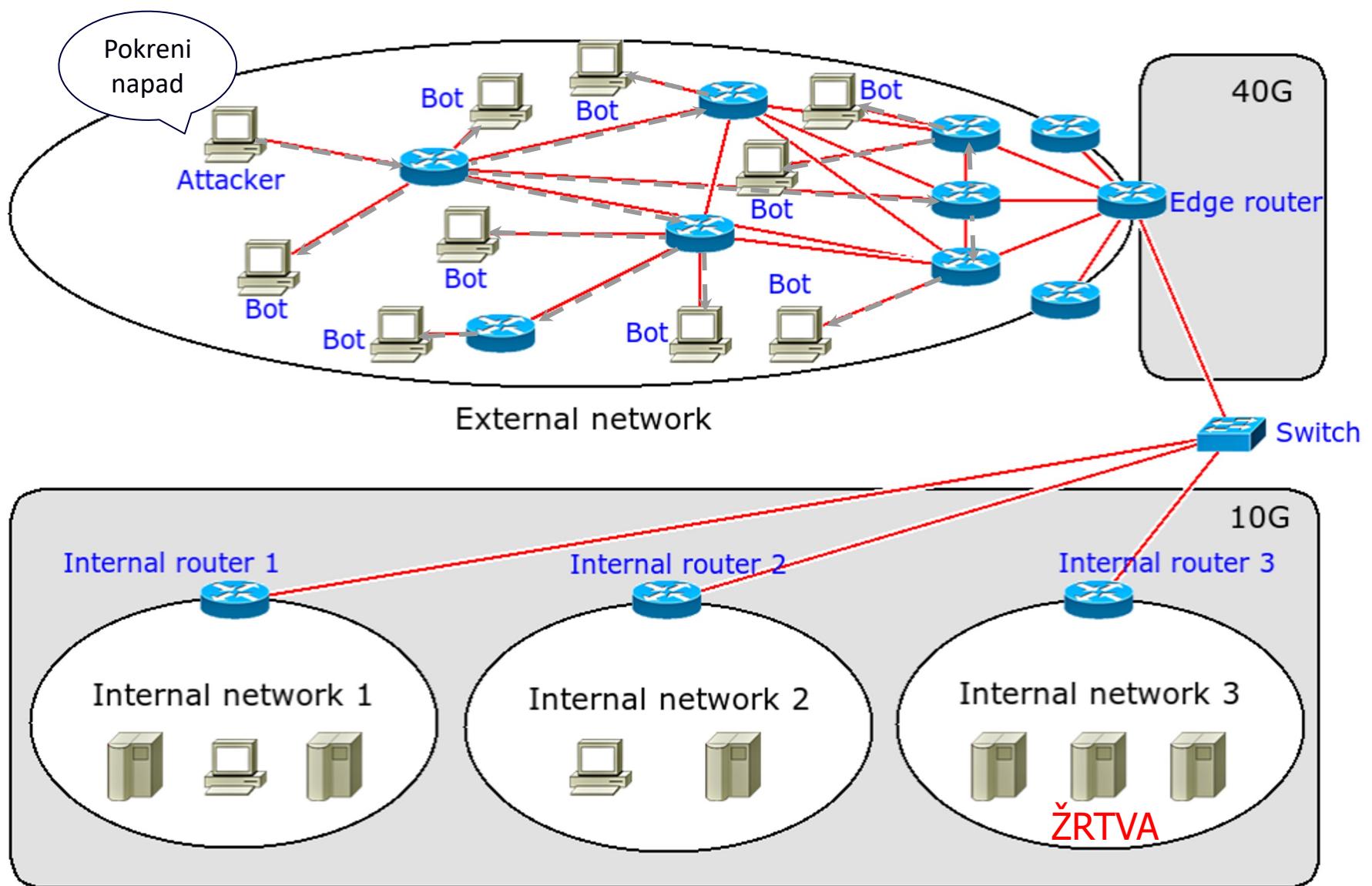
- DoS: Denial of Service / DDoS: Distributed Denial of Service
- nisu specifični za mrežni ili prijenosni sloj
  - bilo koje ograničeno sredstvo može biti cilj napada
    - pristupni link, memorija, CPU, disk, ...
    - cilj napada može biti i nekakva pogreška u aplikaciji ili protokolu
- obrana vrlo teška i ovisi o konkretnom napadu i specifičnostima samog napada
  - u određenim slučajevima nužna je suradnja s ISP-om
  - dobro je unaprijed planirati razne situacije
- posljedice napada mogu biti katastrofalne za žrtvu
  - nedostupnost ima novčane i reputacijske posljedice

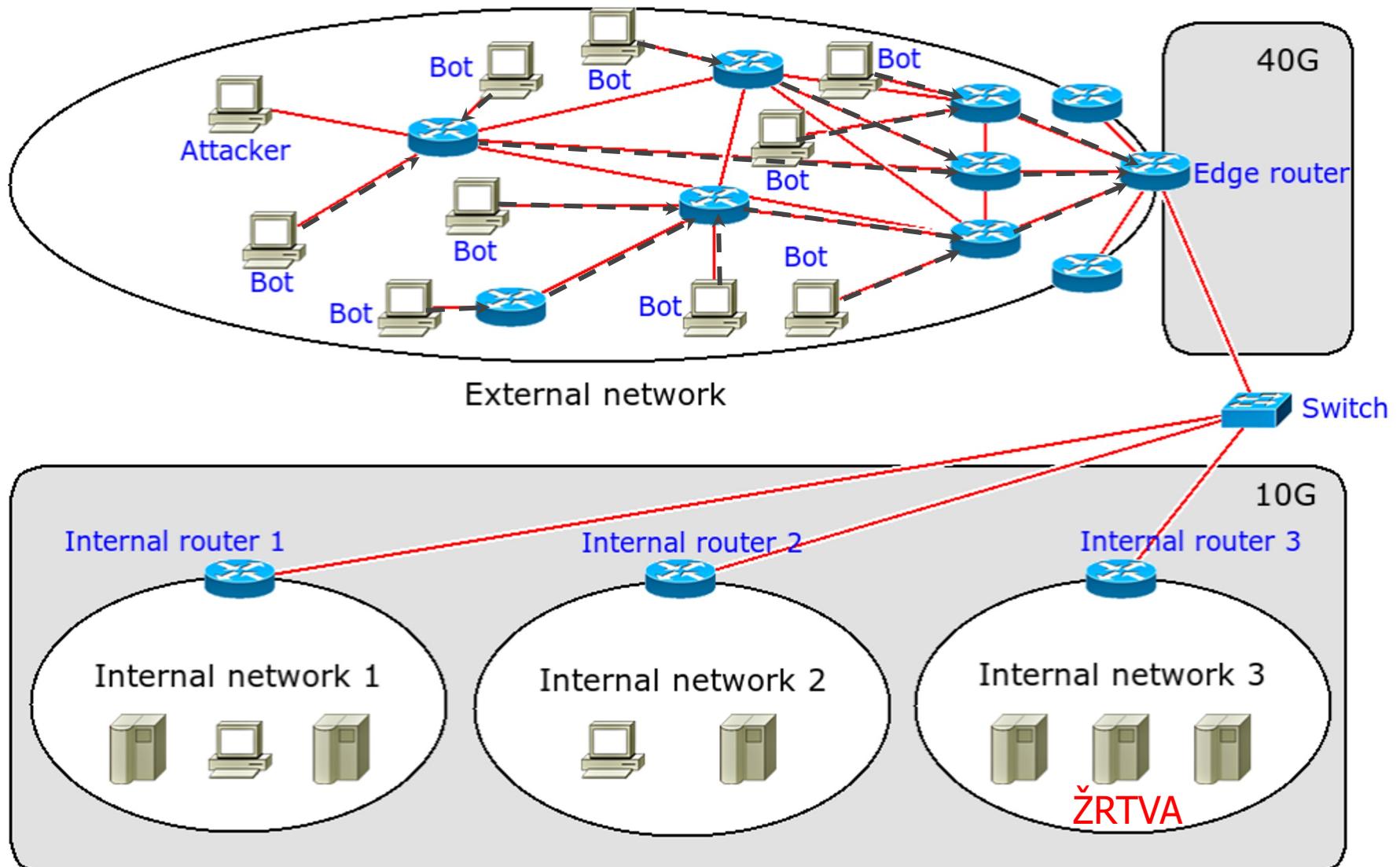
# Mehanizam za provođenje napada

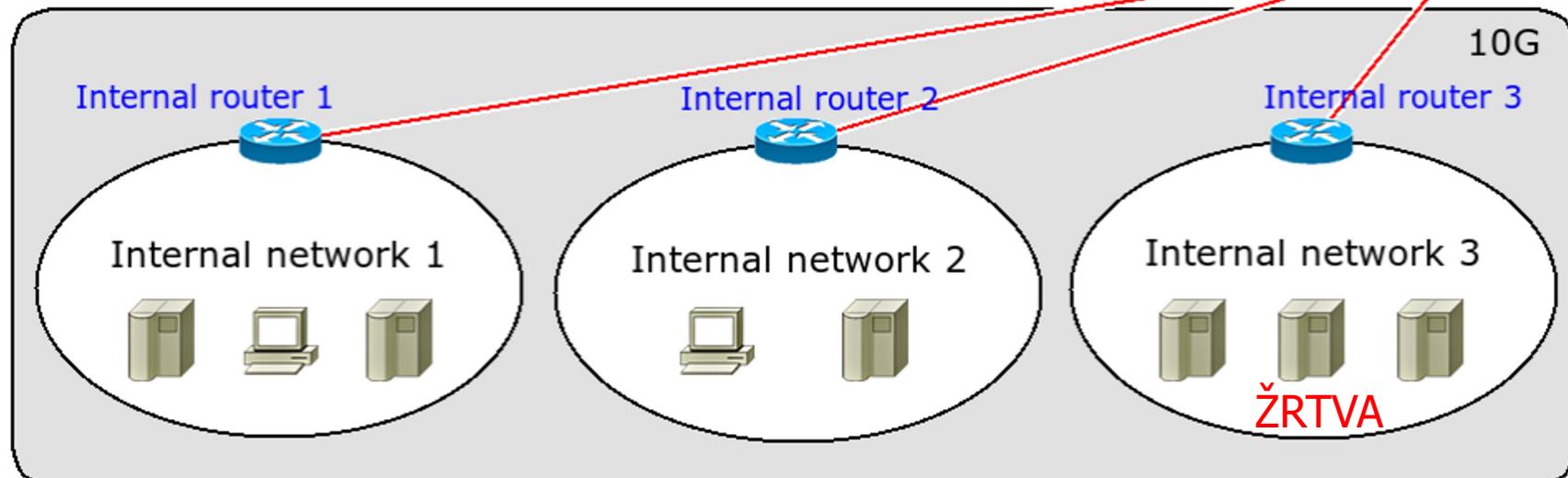
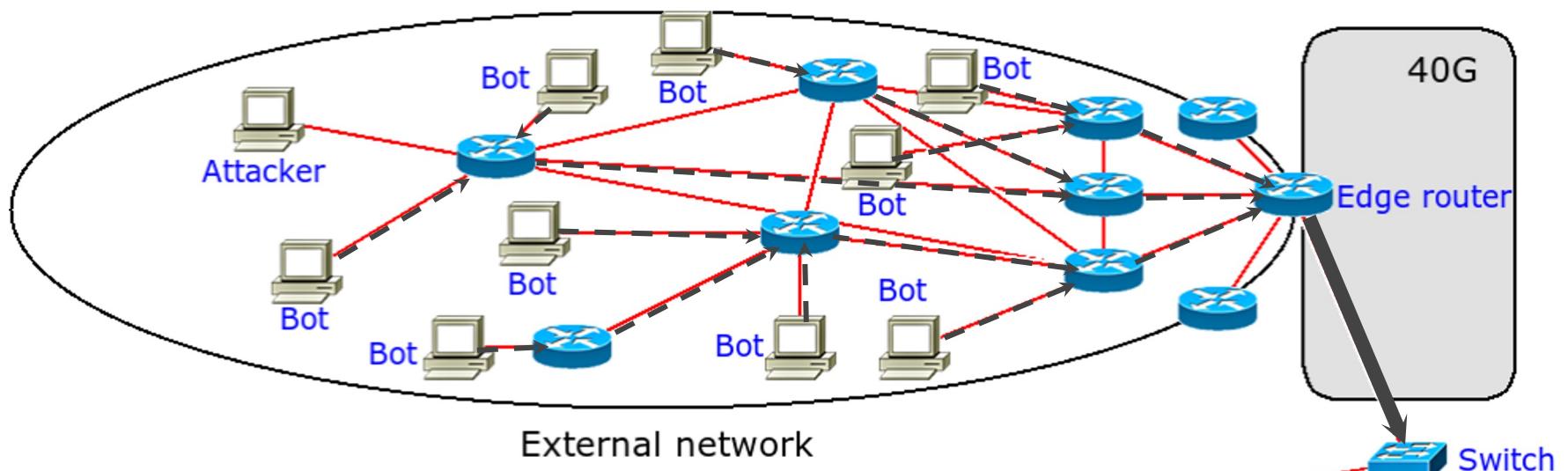
- „botmasteri” zaraze velik broj računala koja tvore „botnet”
  - može biti i više od 100,000 zaraženih računala
  - svako zaraženo računalo se naziva *bot* ili *zombie*
- komunikacija s *botnetom* se odvija preko C&C (Command and Control)
  - komunikacija između zaraženih računala i C&C odvija se putem IRC-a, HTTP-a ili P2P protokolom
- uklanjanje *bota*
  - nije moguće/nema smisla djelovati na pojedina računala
  - napadači su često prikriveni
  - preuzimanje C&C je najčešći način

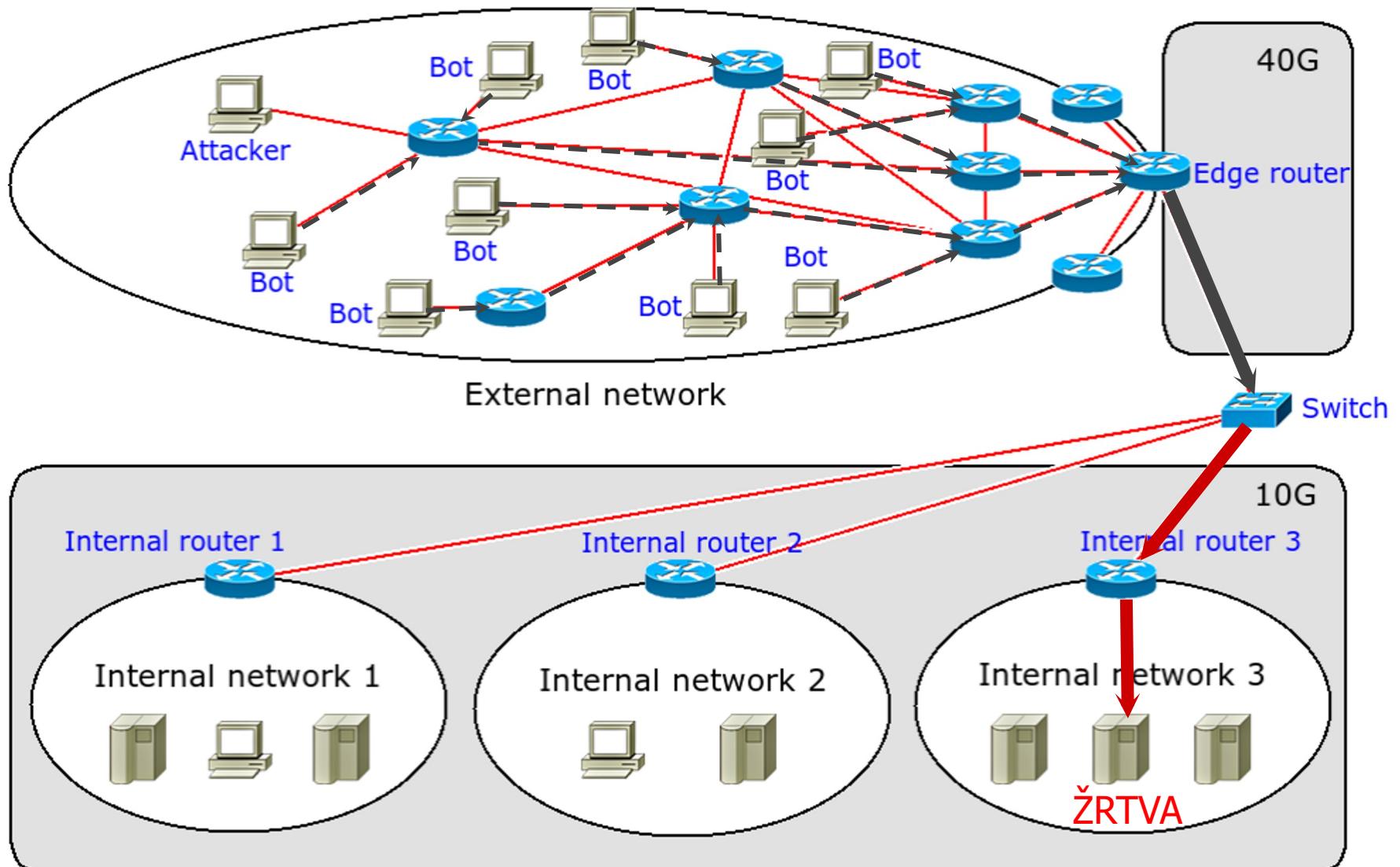
# DDoS napadi (Distributed Denial-of-Service)

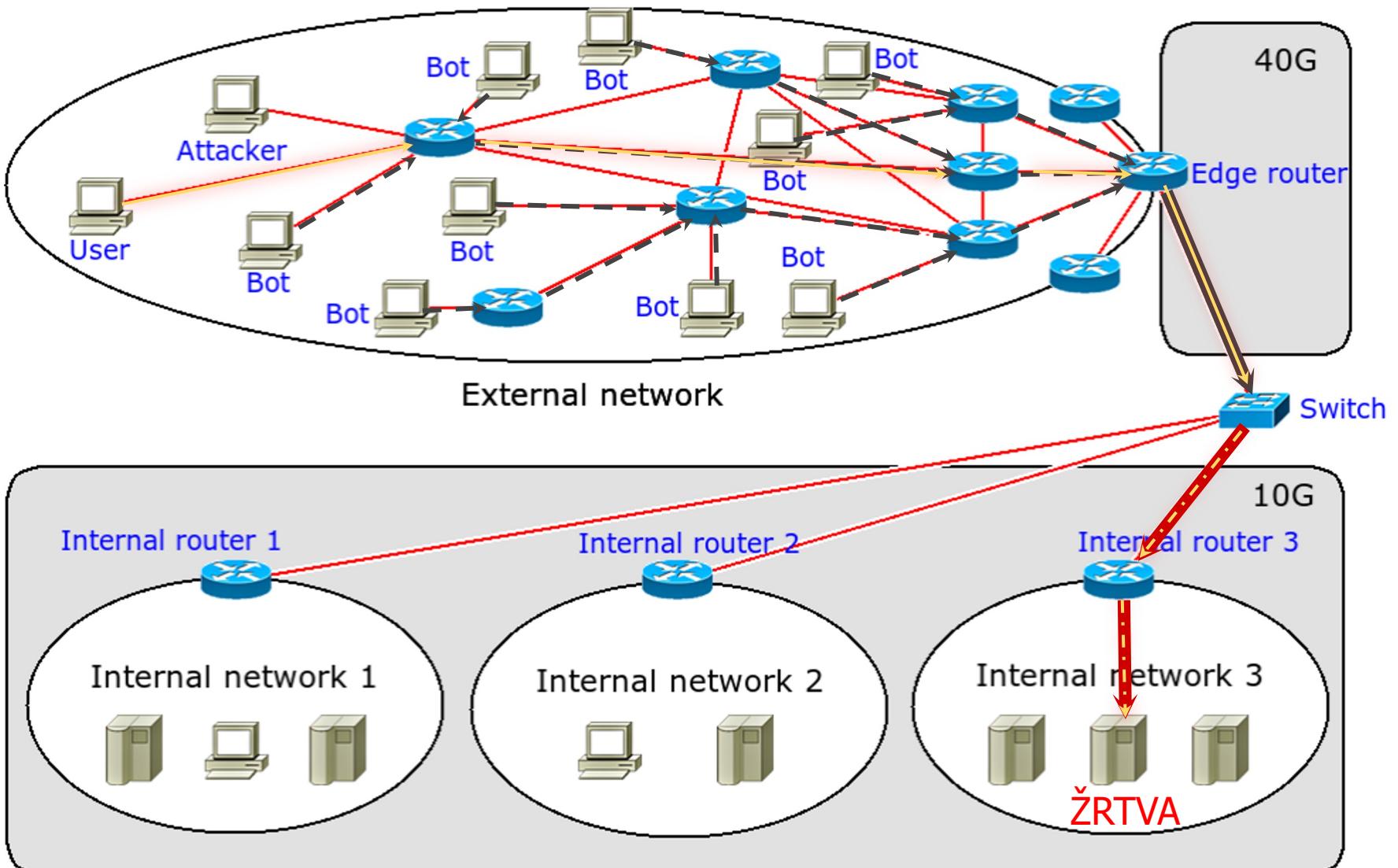












# DDoS napadi (Distributed Denial-of-Service)



2016. – deseci milijuna  
jedinstvenih IP adresa izvorišta  
(623 Gbps; Mirai botnet)



2020. – 2.3 Tbps  
(CLDAP DDoS refl. & amp.)



2020. – 167 Mpps  
spoofanih datagrama prema 180.000  
CLDAP, DNS, SMTP



2018. – 1.35 Tbps  
(memcached; tisuće AS)

Offering	Price
1-day DDoS service	US\$30-70
1-hour DDoS service	US\$10
1-week DDoS service	US\$150
1-month DDoS service	US\$1,200

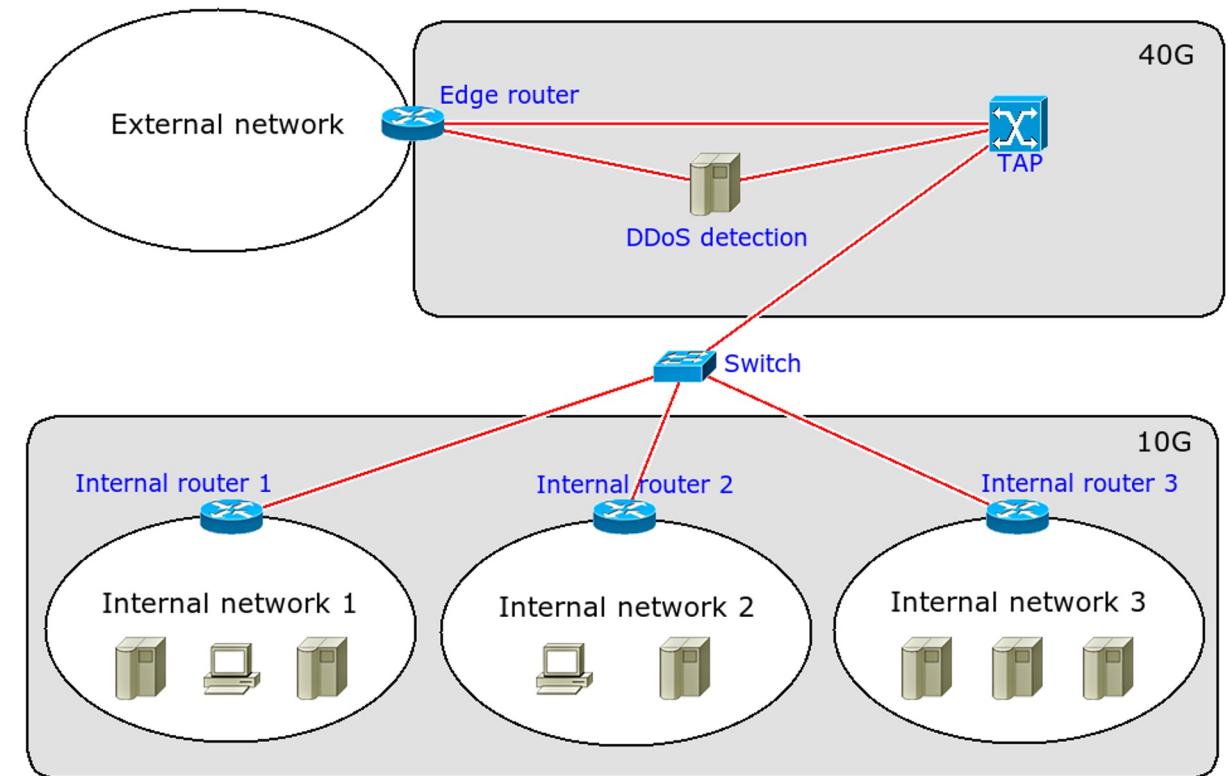
izvor: <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

# Zaštita od volumetričkih uskraćivanja usluge

- promatrani sustav sastoji se od izvora napada, komunikacijskih puteva te žrtve
- obrana je moguća na svakom od tih mesta
- zaštita od napada ovisi o konkretnoj situaciji
  - nužno je dobro poznavanje vlastite infrastrukture i karakteristika napada
  - nužno je uspostaviti dobar odnos sa svojim ISP-om
    - ISP može filtrirati promet na svojim usmjernicima
    - primjer: za napad temeljen na UDP-u moguće je blokirati UDP (pripaziti na DNS koji koristi UDP)
    - primjer: paketi dolaze izvan Hrvatske, moguće blokiranje vanjskog prometa (vatrozid, ili BGP)
- višestruki pristup Internetu
  - korištenje ADSL-a i sličnih metoda
  - korištenje BGP usmjeravanja

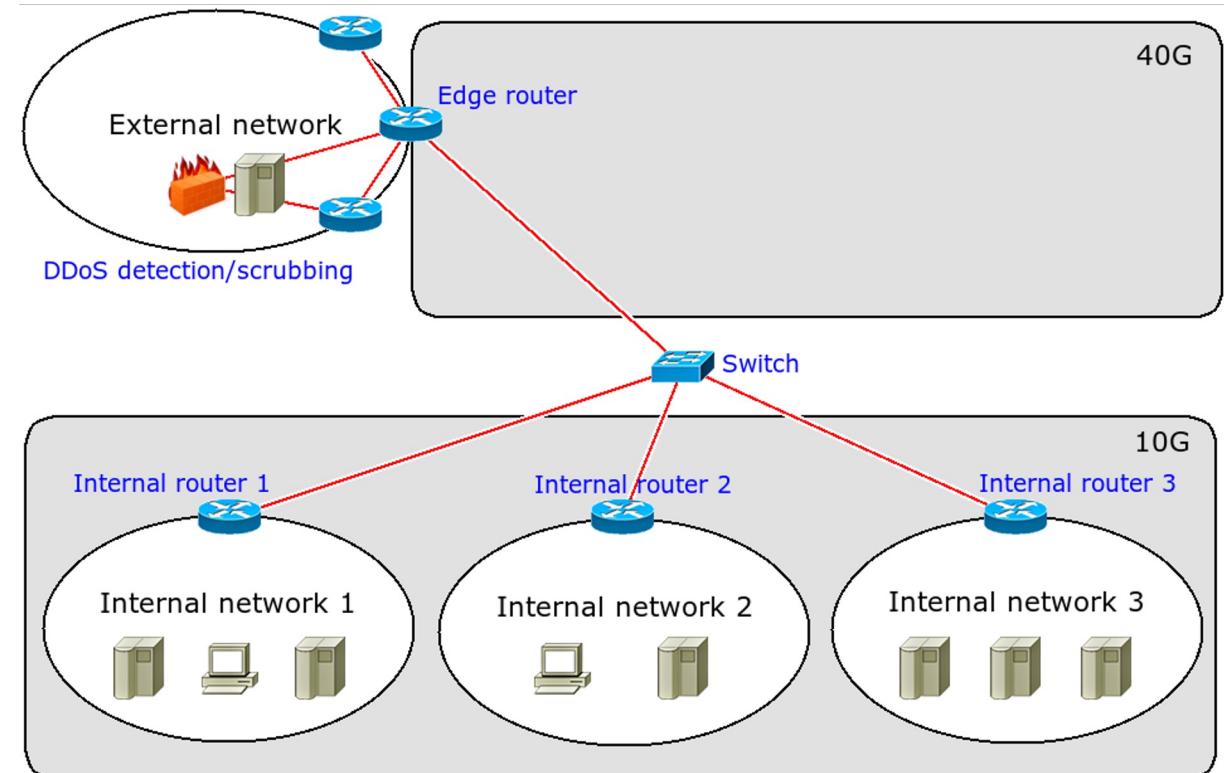
# Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



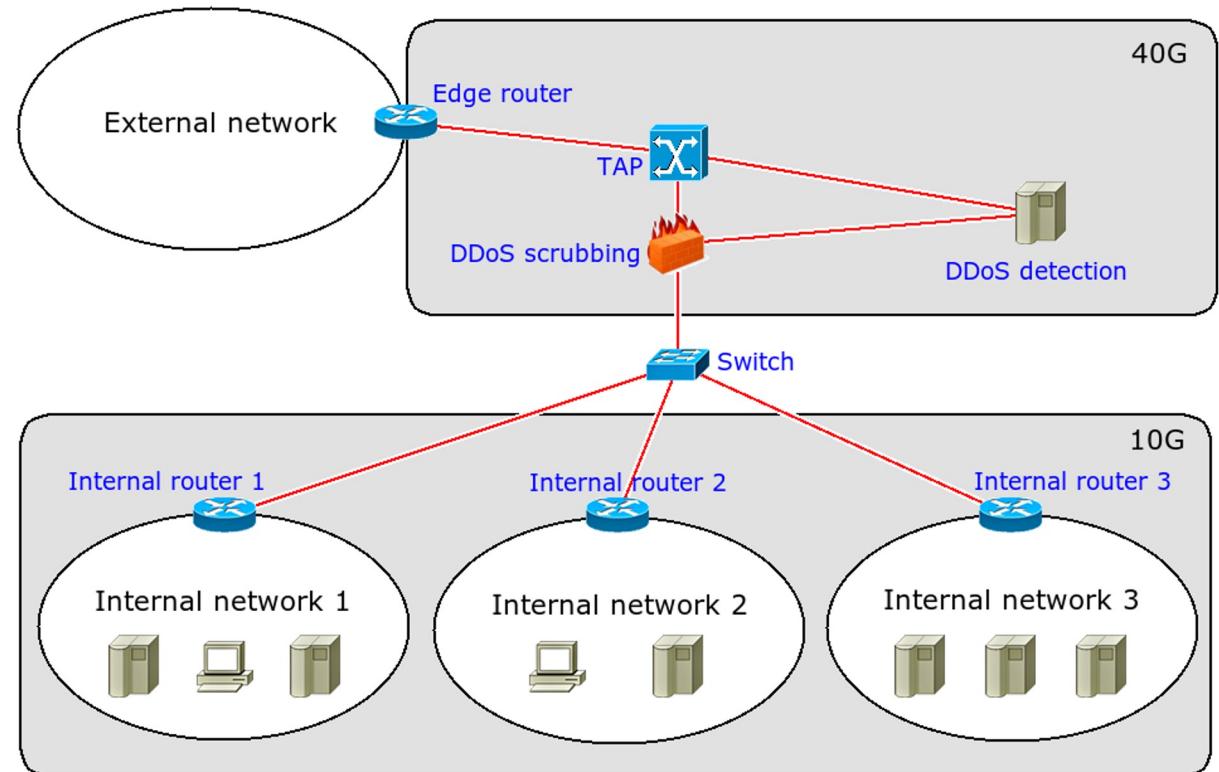
# Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



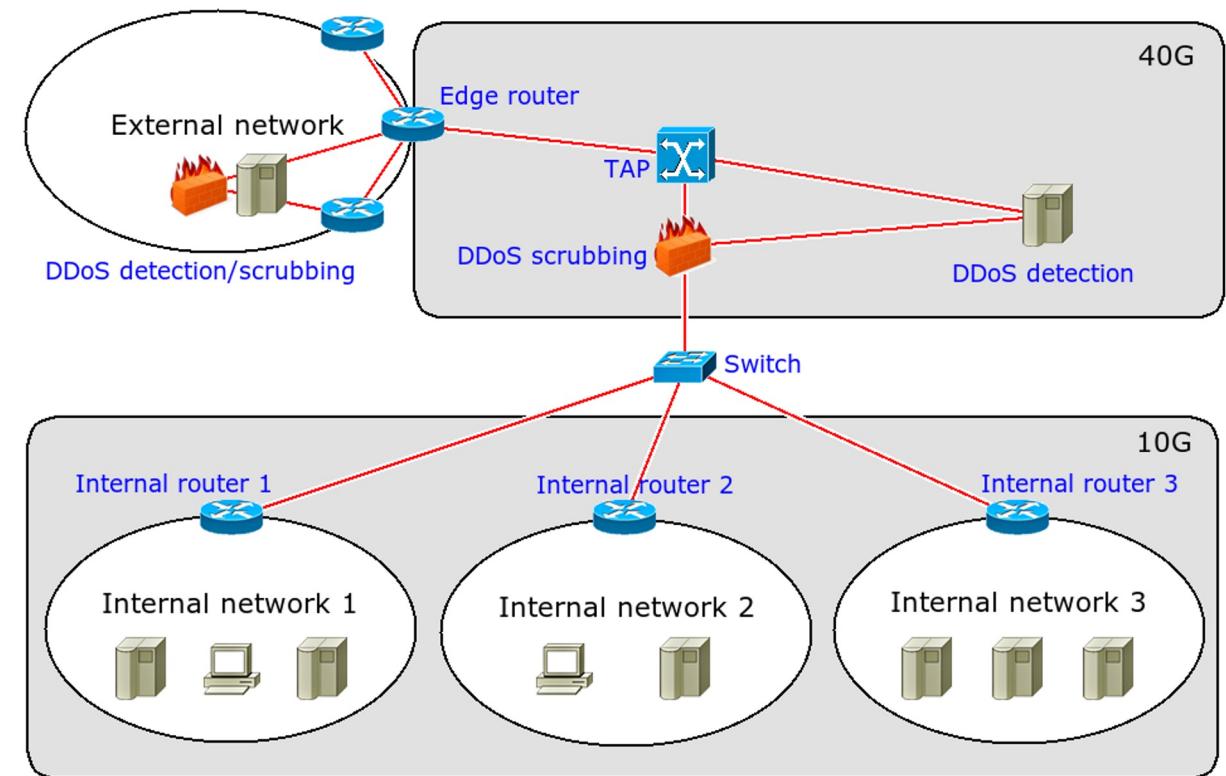
# Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



# Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



# Zaštita od DDoS napada: HW

- ASIC, FPGA (složeno i uglavnom nefleksibilno)
  - teško je modificirati i nadograđivati
  - energetski neučinkovito (TCAM)
  - vlasnička programska podrška (*proprietary*)
  - ograničena memorija
  - skupo!
  - brzo!



AntiDDoS8030



AntiDDoS8080



AntiDDoS8160

izvor: HUAWEI AntiDDoS8000 DDoS Protection System  
<https://carrier.huawei.com/~/media/cnbg/downloads/product/fixed%20network/carrier%2012700/pdf/huawei%20antiddos8000%20ddos%20protection%20system%20datasheet.pdf>

# Zaštita od DDoS napada: SW

- programsko filtriranje
  - fleksibilno, relativno jednostavna modifikacija i nadogradnja
  - jeftino, „off-the-shelf”
  - ne toliko brzo?
- standardni „firewall”
  - iptables, ipfw, ...
  - IPset – hash za pohranu IP adresa
- korišteni programski okviri (*framework*) i tehnologije:
  - netmap
  - eBPF/XDP
  - DPDK – Intel

# 10 Gbps / 40 Gbps / 100 Gbps?

- najmanji ethernet okvir: 84 okteta
  - 7 okteta MAC preambula + 1 oktet „start frame delimiter“
  - eth. adresa odredišta: 6 okteta + eth. adresa izvođača: 6 okteta + tip: 2 okteta
  - minimalni „payload“: 46 okteta
  - CRC: 4 okteta; razmak između ethernet okvira: 12 okteta („inter-frame gap“)
- najveći ethernet okvir: 1538 okteta,  $(12) + (7+ 1) + (6 + 6 + 2)$  + MTU je  $1500 + 4$
- ako se koristi danas standardna mreža brzine 10 Gbit/s, za najmanji ethernet okvir:

$$\frac{10 \cdot 10^9 \text{ bit/s}}{84 \text{ okteta} \cdot 8 \text{ bita}} = 14.880.952 \text{ pps (packets per second)} = 14,88 \text{ Mpps}$$

- vrijeme dostupno za obradu svakog paketa pri brzini 14.88 Mpps:  $\frac{1}{14.880.952} = 67,2 \text{ ns}$
- ako CPU radi na 3 GHz i izvodi samo jednu instrukciju po ciklusu: 201 CPU ciklus po paketu
- 100 Gbps, 148,8 Mpps, CPU 4 Ghz: ~27 CPU ciklusa po paketu
- „cache-misses“: 32 ns; vrijeme pristupa L2: 4,3 ns; vrijeme pristupa L3: 7,9 ns; sistemski poziv na Linuxu: minimalno 41,85 ns

# Usluge zaštite specijaliziranih tvrtki (1)

- na tržištu postoje specijalizirane tvrtke koje pružaju zaštitu
  - Akamai, CenturyLink, CloudFlare, DOSarrest, F5 Networks, Incapsula, Level3, Neustar, Verisign, cratis.hr
  - opće naziv: „DDoS Protection Service – DPS”
- usluga nije samo protiv volumetričkih napada već i semantičkih
- dva temeljna načina implementacije tih usluga
  - zaštita se nalazi u oblaku
  - u mrežu klijenta instalira se uređaj za zaštitu
  - hibridni pristup kombinira oblak i uređaj u mreži klijenta

# Usluge zaštite specijaliziranih tvrtki (2)

- način korištenja usluga DPS-a: DNS i BGP
- promjene u DNS i primjena reverznog posredničkog poslužitelja (proxy)
  - prikladno za pojedine Web stranice/portale
  - kada je moguće koristiti reverzni posrednički poslužitelj
- korištenjem protokola BGP tvrtka za zaštitu šalje obavijesti o mreži klijenta
  - promet stiže do DPS-a, filtrira se te se tunelima šalje do klijenta
  - prikladno za zaštitu cijelih mreža ili kada reverzni posrednički poslužitelj nije moguće koristiti

# Taksonomija DDoS napada (UDP)

- RioRey: „Taxonomy of DDoS Attacks”  
<https://www.riorey.com/types-of-ddos-attacks/>
- UDP:
  - UDP Flood
  - Fragmentation
  - DNS Flood
  - VoIP Flood
  - Media Data Flood
  - Non-Spoofed UDP Flood

## *UDP amplification, UDP reflection*

- servisu koji koristi UDP (bez autentifikacije) pošalje se upit s lažiranom izvorišnom adresom a njegov odziv sadrži više podataka od upita
- “UDP-Based Amplification Attacks”
  - <https://www.us-cert.gov/ncas/alerts/TA14-017A>
- “Weaponizing Middleboxes for TCP Reflected Amplification”
  - <https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/>

# Primjeri *UDP amplification, UDP reflection*

- „DNS amplification” - 28 do 54 puta
- „NTP amplification” – 556.9 puta
  - Network Time Protocol – protokol za sinkronizaciju vremena
  - loša konfiguracija omogućava slanje upita poslužitelju o posljednjih 600 sinkroniziranih računala
- „SNMP amplification” – teoretski do 650 puta
- SSDP - 30.8 puta
- CharGEN - 358.8 puta

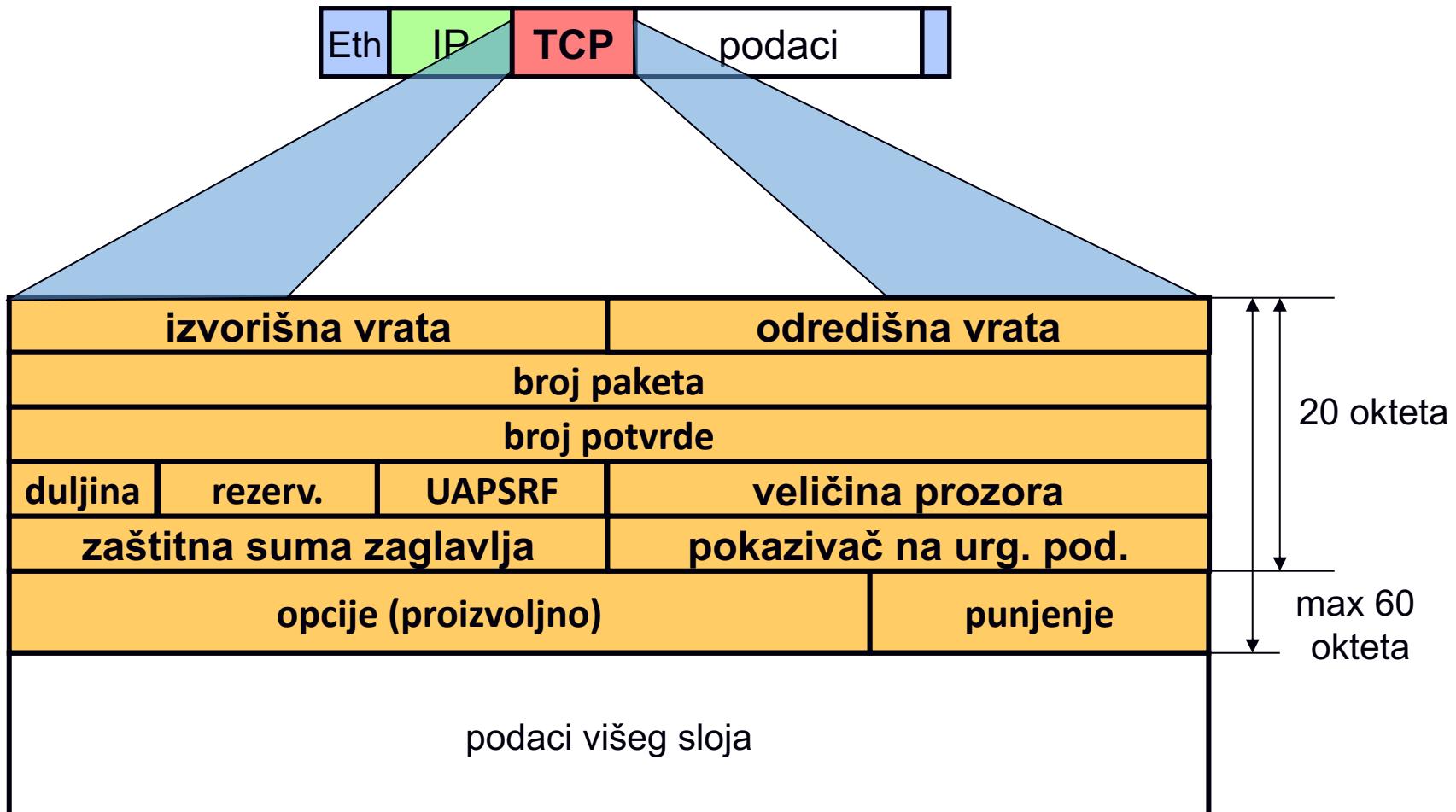
# Primjeri *UDP amplification, UDP reflection*

- akamai's [state of the internet] / security Q2 2016 report
  - <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf>
  - <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf>
- DDoS korištenjem DNS
  - 2012. godine, 65 Gbit/s
  - 2013. godine, 300 Gbit/s
- DDoS korištenjem NTP (Network Time Protocol)
  - 2014. godine, 100 Gbit/s
  - 2014. godine, 400 Gbit/s (CloudFlare)

# Protokol TCP

- Koneksijski (spojno) orijentirani transportni protokol
- Pouzdan
  - istek vremenske kontrole (*timeout*) i retransmisija
  - potvrde
  - nema duplicitiranja
  - slaže pakete
  - kontrolni zbroj
  - omogućuje kontrolu toka
- Obostrana veza

# Format TCP segmenta



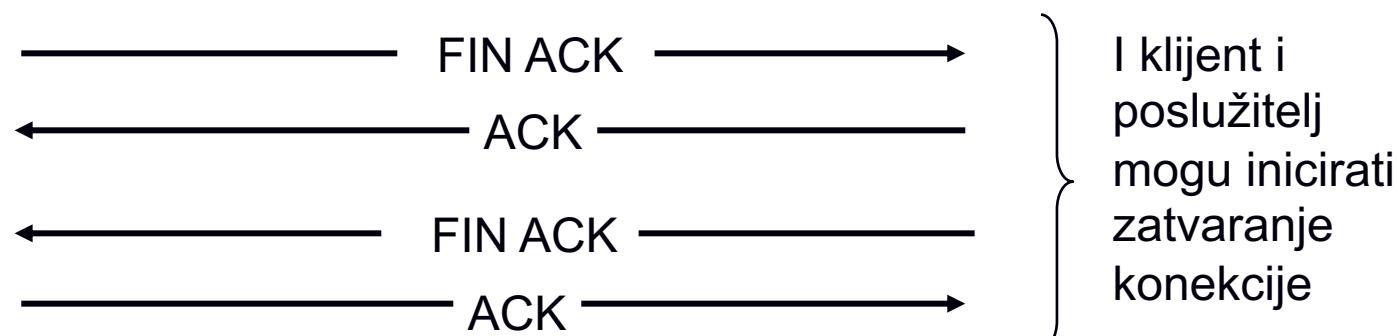
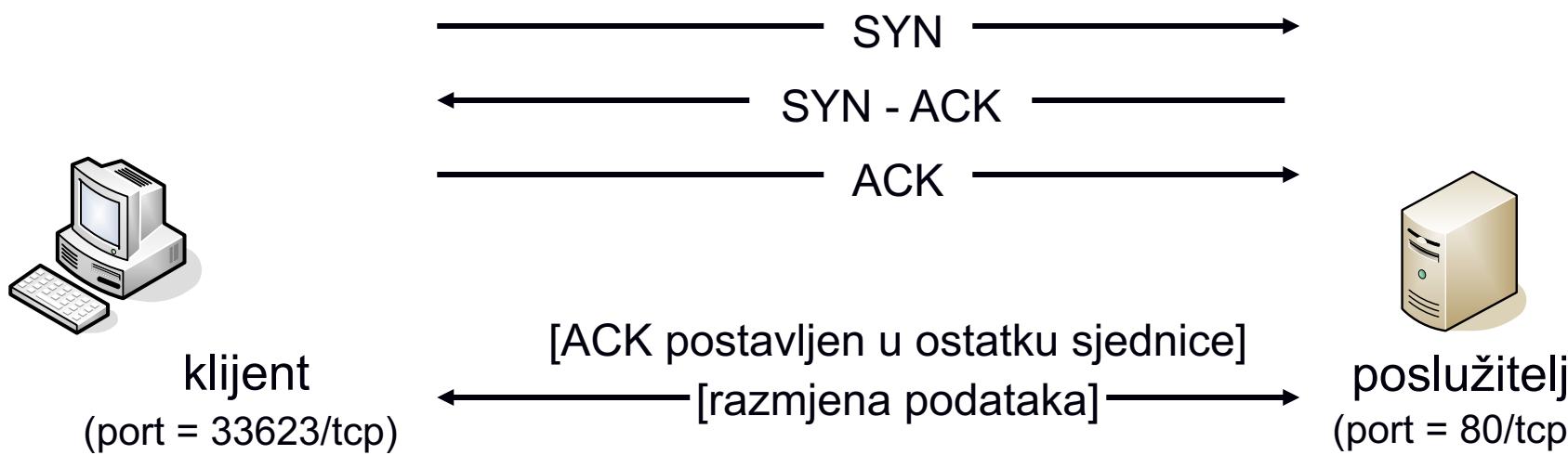
# Slijedni brojevi i brojevi potvrde

- SEQ
  - slijedni broj (*„Sequence number”*)
  - označava redni broj prvog okteta koji se prenosi u korisničkim podacima
- ACK
  - broj potvrde (*„Acknowledgment number”*)
  - označava redni broj okteta koji pošiljatelj ove potvrde očekuje primiti
  - ujedno potvrđuje da su svi podaci do tog okteta primljeni

# TCP zastavice

- SYN dogovaranje početnih brojeva pri uspostavi veze
- FIN završeno slanje podataka
- ACK broj potvrde je postavljen
- URG postavljen je „*urgent pointer*”
- PSH primatelj treba predati podatke aplikaciji što je prije moguće
- RST resetira vezu

# Primjer TCP sjednice



# Slanje podataka i kontrola toka

- u paketu se šalje potvrda o zadnjim ispravno primljenim podacima
- paket se prihvata samo ako je unutar veličine predajnog prozora („transmission window”)
- za potvrdu se može koristiti i prazni segment (segment bez podataka)
- paketi sa zastavicama SYN ili FIN povećavaju slijedni broj iako ne sadrže podatke
- protokol kliznog prozora („Sliding Window Protocol”)
  - omogućava slanje više paketa prije nego što dođe potvrda o prispjeću paketa
  - veći protok podataka u odnosu na protokol „stop-and-wait”

# Napadi na protokol TCP

- za napad je bitan položaj napadača
- na putu kojim prolaze TCP segmenti (engl. on path)
  - MITM napad, napadač može pratiti i mijenjati komunikaciju
  - jedina potpuna zaštita je IPsec
  - TLS ne štiti od napada uskraćivanja usluge
- van puta kojim prolaze TCP segmenti (engl. off path)
  - napadač ne može pratiti komunikaciju i mora pogoditi određene parametre
  - manje mogućnosti napada, ali s propusnošću veze raste prijetnja

# Taksonomija DDoS napada (TCP)

- RioRey: „Taxonomy of DDoS Attacks”  
<https://www.riorey.com/types-of-ddos-attacks/>
- TCP:
  - SYN Flood
  - SYN-ACK Flood
  - ACK&PUSH Flood
  - Fragmented ACK
  - RST or FIN Flood
  - Synonymous IP
  - Fake Session
  - Session Attack
  - Missused Application

# Napad TCP SYN flood (1)

- Poslužitelj po primitku SYN segmenta rezervira resurse
  - veza je u poluotvorenom stanju koje traje neko vrijeme
  - dopušten je samo određen broj poluotvorenih veza
- "Problem" za napadača
  - Računalo koje primi SYN+ACK, a nije poslalo SYN, odgovara s RST
  - Napadač mora koristiti adresu s koje neće stići odgovor!

# Napad TCP SYN flood (2)

```
$ netstat -anf inet
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	0	10.0.1.10.22	192.168.1.182.11008	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.225.28014	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.175.44828	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.184.28987	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.0.10303	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.237.25561	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.186.48231	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.53.20148	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.14.60914	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.68.35857	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.74.57236	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.156.2794	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.217.59919	SYN_RCVD

...

- CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
- Defining Strategies to Protect Against TCP SYN Denial of Service Attacks
  - <https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/14760-4.html>

# Napad TCP SYN flood (3)

- Ne postoji standardizirana niti potpuna zaštita
- Neke metode zaštite
  - Povećanje broja dozvoljenih poluotvorenih veza
  - Skraćenje trajanja poluotvorene veze
  - Smanjenje količine stanja poluotvorene veze (SYN cache)
- Zaštita uz pomoć kolačića (SYN cookies)
  - Za inicijalni SYN se uopće ne čuva stanje
    - Stanje se rekonstruira iz završnog odgovora
  - “kolačić” je posebno odabran 32 bitni slijedni broj
    - ISN klijenta, MSS klijenta, vremenski brojač, adresa i pristup

# Napad TCP SYN flood (4)

- Zaštita uz pomoć kolačića (nastavak)
  - Problem nedovoljne količine prostora u TCP zaglavljiju
  - Niz opcija nije podržan, primjerice skaliranje prozora, različite veličine MSS-a (3 bita)
- SYN napad je lekcija za sve novije protokole
- Amplificirani napad
  - Poslužitelju se šalje SYN segment s lažiranom adresom žrtve
  - Server obavlja retransmisiju SYN+ACK segmenta

# Primjer TCP DDoS napada

- „Record-breaking DDoS reportedly delivered by >145k hacked cameras”
  - <http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-delivers-internets-biggest-ddos-ever/>
  - rujan 2016.
  - 145607 kamere / dvr (1-30 Mbps po IP)
  - > 1.5 Tbps DDoS
  - tcp/ack, tcp/ack+psh, tcp/syn

# RST i FIN napadi na protokol TCP

- Prema TCP specifikaciji po primitku ispravnog RST segmenta potrebno je raskinuti vezu
- RST napad
  - Slanje segmenta s postavljenom RST zastavicom
  - Problem je pogoditi parametre TCP veze
    - sljedni broj (unutar prozora!), izvorišna i odredišna IP adresa, izvorišni i odredišni pristup (port)
    - 1Mbps, MSS=1500, 100ms latencije, 15 skokova, WIN 35000
    - 1:57000, 40 okteta RST, 20s (na 1Mbps)
    - za 16384 pristupa, 91 sat
- FIN napad
  - Sličan RST napadu jedino se zatvara pojedini kraj veze

# Zaštita od RST i FIN napada

- TCP MD5/AO
- (Ručno) ograničenje maksimalne veličine prozora
  - Napadač u tom slučaju mora napraviti više pokušaja
- Ograničenje slijednog broja u RST segmentima
  - Dodatno slanje ACK segmenta
- Druga rješenja koja modifciraju ponašanje TCP-a

# ICMP napadi na protokol TCP

- ICMP je mrežni protokol
  - Na temelju podataka iz višeg sloja se obavlja demultiplexiranje
    - Zaglavje mrežnog sloja i prvi 64 bita višeg sloja [RFC793]
    - Što više podataka, ali manje od 576 okteta [RFC1812]
- Konkretni napadi
  - ICMP poruke o greškama uzrokuju prekid veze
  - Port ili protokol nedostizni, fragmentacija potrebna a DF bit postavljen
  - ICMP poruka o zakrčenju (ICMP Source Quench)
- Zaštita prijenosnog sloja
  - Provjera ispravnih slijednih brojeva

# Sigurnosna rješenja

- TCP-MD5 (RFC2385) / TCP-AO (RFC5925)
  - Uglavnom za zaštitu protokola BGP
    - BGP koristi i TTL zaštitu
  - Valjani RST, kada nema druge strane, će biti ignoriran
  - Problematično zbog dijeljene tajne, kripto-algoritmi usporavaju poslužitelje/usmjernike,
  - TCP MD5 zamijenjen s TCP AO jer koristi problematičan algoritam, nema zaštite od ponavljanja, ne podržava IPv6, zamjena dijeljene tajne je problematična (nema načina signalizacije promjene dijeljene tajne)
- IPsec – lako potpuno, nije skalabilno rješenje
- TLS

# TCP „reflected amplification attack”?

- TCP uspostavlja vezu (3-way handshake)
- „IP spoofing“ se može koristiti samo za napade tipa SYN-flood?
- „Weaponizing Middleboxes for TCP Reflected Amplification“
  - <https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/>



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

Digitalni certifikati



# Creative Commons



- **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.

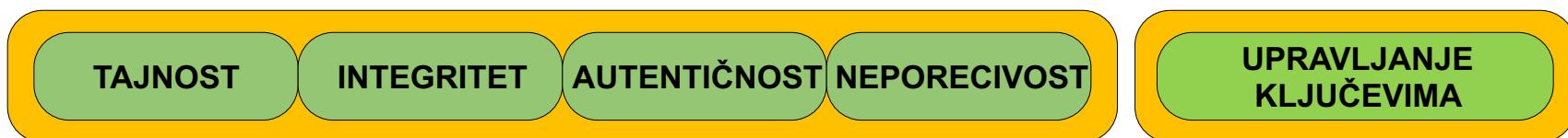


U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci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

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

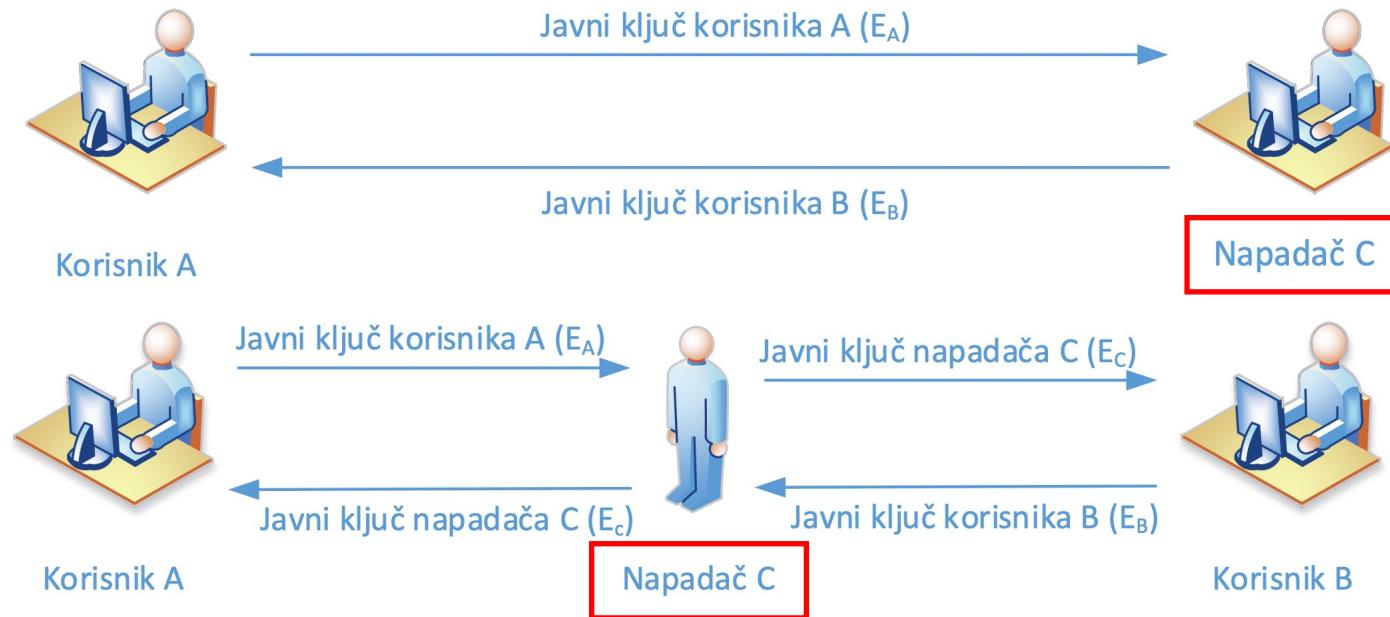
# Ponovimo ...

- simetrični algoritmi
  - jedan tajni ključ (za šifriranje i dešifriranje koristi se isti ključ)
- asimetrični algoritmi:
  - par ključeve
  - javni ključ dostupan svima
  - privatni ključ dostupan samo vlasniku
- upravljanje ključevima



# Problem sigurne distribucije javnih ključeva

- Kad primimo nečiji javni ključ kako znamo da nam netko nije podmetnuo svoj javni ključ?
  - Kako znamo da nije u tijeku MITM napad ili lažno predstavljanje? Javni ključ je samo jedan veliki broj...
  - Prva slika prikazuje lažno predstavljanje, a druga MITM napad



# Problem sigurne distribucije javnih ključeva

- temelj rješenja čini certifikacijsko tijelo (engl. certificate authority, CA)
  - treća strana kojoj svi vjeruju (engl. trusted third party)
- javnim ključevima dodaju se informacije o identitetu vlasnika koje potom potpisuje certifikacijskog tijelo
  - korisnik (osoba, Web stranica, poslužitelj elektroničke pošte) koji želi certifikat generira javni i tajni ključ, javnom ključu dodaje identifikacijske podatke i potpisuje ih te šalje certifikacijskom tijelu na potpis
    - Certificate Signing Request, CSR
  - CA prije potpisivanja mora provjeriti da javni ključ doista pripada onome čiji identitet je dan uz javni ključ (telefonski, direktno, ...)
  - javni ključ, podaci o identitetu i potpis CA čine certifikat

# Problem sigurne distribucije javnih ključeva

- certifikacijsko tijelo također ima svoj certifikat
  - njega potpisuje samo certifikacijsko tijelo
    - samopotpisani certifikat (engl. self-signed certificate)
  - moraju ga imati svi na Internetu i tada će biti u mogućnosti provjeriti svaki certifikat koji je CA potpisao te na taj način spriječiti MITM napade i lažno predstavljanje
- tako povezani javni ključevi čine infrastrukturu javnog ključa (engl. Public Key Infrastructure, PKI)

# Upravljanje ključevima

- upravljanje ključevima (engl. key management)
  - kriptografski algoritmi su opisani standardima
  - upravljanje ključevima je složeniji dio kriptografskog sustava; skup ljudi, hardvera, softvera, procedura, standarda i politika koji treba riješiti sljedeće probleme:
    - kreiranje
    - distribucija
    - korištenje
    - arhiviranje
    - automatizacija životnog ciklusa ključa
- 20% tehnologija : 80% procedure
- PKI (Public Key Infrastructure) - infrastruktura javnog ključa

# PKI

- Ima li privatni ključ samo odgovarajuća osoba?
  - kriptografski uređaj
- Kako povezati javni ključ sa osobom?
  - certifikat
- Vrijedi li nečiji javni ključ? Da li je opozvan?
  - lista opozvanih certifikata - CRL
- Tko će izdati i jamčiti za certifikat?
  - certifikacijsko tijelo – certification authority – CA
- Tko će jamčiti identifikaciju i autentifikaciju osobe?
  - registracijsko tijelo – RA
- Kako dobiti / distribuirati javni ključ ?
  - javni imenik
- U koju svrhu mogu koristiti ovaj certifikat?
  - certificate policy - CP

# Javni ključ

- javni ključ / Public-Key: (1024 bit)

Modulus:

```
00:ca:a4:05:83:6f:0c:1d:a0:3e:2d:93:89:d2:76:  
2d:25:9e:b4:c4:81:09:e9:f3:e4:c5:0f:12:88:91:  
a7:f0:ac:21:3a:e6:f1:22:5d:f7:9e:84:e0:94:23:  
b2:02:00:61:40:fb:ac:5f:e3:25:dc:7a:3f:94:e9:  
b4:82:ac:88:da:20:6f:a8:42:d3:bd:2e:bc:b4:ef:  
ce:0b:22:06:22:84:51:74:ac:15:62:d0:dd:78:f7:  
7e:71:86:32:35:2c:07:3e:97:7e:f1:8f:13:2b:78:  
36:eb:9a:9e:ee:a4:0a:cb:23:b5:05:96:e6:c8:ce:  
b8:1e:18:1e:df:62:6d:74:89
```

Exponent: 65537 (0x10001)

- kako povezati javni ključ s korisnikom (subjektom)?
  - javni ključ nema podatke o osobi kojoj pripada
- zahtjev: prepoznatljivost i jednostavno korištenje javnog ključa
  - digitalni certifikat

# Digitalni certifikati

- Certifikat – digitalni objekt
  - Sadrži javni ključ i ostale informacije o subjektu, izdavatelju i valjanosti
  - Subjekt certifikata je naziv računala ili osobe kojoj certifikat pripada
  - Certifikat izdaje i digitalno potpisuje izdavatelj certifikata (CA, Certificate Authority)
- Standardi:
  - format X.509 - ISO, ITU-T
  - RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

# Sadržaj osobnog certifikata



DN: cn=Anja Kovač, o=FER  
c=HR

Serial #: 3913133

Start: 6-7-2009 3:33

End: 6-7-2010 3:33

CRL: cn=CRL2, o=FER, c=HR

Key:



CA DN: o=UNI-ZG,  
c=HR



informacije o korisniku:  
ime, institucija, država (ili naziv poslužitelja)

jednoznačni serijski broj

informacija o važenju certifikata

informacija o povlačenju certifikata

javni ključ korisnika

informacija o instituciji  
koja je izdala certifikat

digitalni potpis institucije  
koja je izdala certifikat

# Sadržaj certifikata za web poslužitelj



The screenshot shows a certificate chain viewer with the following structure:

- USERTrust RSA Certification Authority
- └ GEANT OV RSA CA 4
- └ \*.fer.unizg.hr

Below the tree view, details for the \*.fer.unizg.hr certificate are displayed:

**\*.fer.unizg.hr**  
Issued by: GEANT OV RSA CA 4  
Expires: Sunday, 22 May 2022 at 01:59:59 Central European Summer Time  
✓ This certificate is valid

Navigation links:  
➤ Trust  
➤ Details

# Sadržaj certifikata

**Subject Name** \_\_\_\_\_

**Country or Region** HR  
**Postcode** 10000  
**County** Grad Zagreb  
**Locality** Zagreb  
**Street Address** Unska 3  
**Organisation** Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva  
**Organisational Unit** CIP  
**Common Name** \*.fer.unizg.hr

**Issuer Name** \_\_\_\_\_

**Country or Region** NL  
**Organisation** GEANT Vereniging  
**Common Name** GEANT OV RSA CA 4

**Serial Number** 00 9F 6E AB 25 65 BB F2 CC 7D 8C E0 15 6F 1A FC 4F  
**Version** 3  
**Signature Algorithm** SHA-384 with RSA Encryption ( 1.2.840.113549.1.1.12 )  
**Parameters** None

**Not Valid Before** Thursday, 21 May 2020 at 02:00:00 Central European Summer Time  
**Not Valid After** Sunday, 22 May 2022 at 01:59:59 Central European Summer Time

**Public Key Info** \_\_\_\_\_

**Algorithm** RSA Encryption ( 1.2.840.113549.1.1.1 )  
**Parameters** None  
**Public Key** 256 bytes: A6 05 99 6E EE 6E 2A F6 ...  
**Exponent** 65537  
**Key Size** 2.048 bits  
**Key Usage** Encrypt, Verify, Wrap, Derive  
**Signature** 512 bytes: 5E 5A 3B 65 A1 53 11 20 ...

**Extension** Key Usage ( 2.5.29.15 )  
**Critical** YES  
**Usage** Digital Signature, Key Encipherment

**Extension** Basic Constraints ( 2.5.29.19 )  
**Critical** YES  
**Certificate Authority** NO

**Extension** Extended Key Usage ( 2.5.29.37 )  
**Critical** NO  
**Purpose #1** Server Authentication ( 1.3.6.1.5.5.7.3.1 )  
**Purpose #2** Client Authentication ( 1.3.6.1.5.5.7.3.2 )

# Sadržaj certifikata

<b>Extension</b>	Subject Alternative Name ( 2.5.29.17 )
<b>Critical</b>	NO
<b>DNS Name</b>	*.fer.unizg.hr
<b>DNS Name</b>	fer.unizg.hr
<b>Extension</b>	Certificate Policies ( 2.5.29.32 )
<b>Critical</b>	NO
<b>Policy ID #1</b>	( 1.3.6.1.4.1.6449.1.2.2.79 )
<b>Qualifier ID #1</b>	Certification Practice Statement ( 1.3.6.1.5.5.7.2.1 )
<b>CPS URI</b>	<a href="https://sectigo.com/CPS">https://sectigo.com/CPS</a>
<b>Policy ID #2</b>	( 2.23.140.1.2.2 )
<b>Extension</b>	CRL Distribution Points ( 2.5.29.31 )
<b>Critical</b>	NO
<b>URI</b>	<a href="http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl">http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl</a>
<b>Extension</b>	Embedded Signed Certificate Timestamp List ( 1.3.6.1.4.1.11129.2.4.2 )
<b>Critical</b>	NO
<b>SCT Version</b>	1
<b>Log Operator</b>	Google
<b>Log Key ID</b>	46 A5 55 EB 75 FA 91 20 30 B5 A2 89 69 F4 F3 7D 11 2C 41 74 BE FD 49 B8 85 AB F2 FC 70 FE 6D 47
<b>Timestamp</b>	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
<b>Signature Algorithm</b>	SHA-256 ECDSA
<b>Signature</b>	72 bytes: 30 46 02 21 00 98 A1 CF ...

<b>SCT Version</b>	1
<b>Log Operator</b>	Let's Encrypt
<b>Log Key ID</b>	DF A5 5E AB 68 82 4F 1F 6C AD EE B8 5F 4E 3E 5A EA CD A2 12 A4 6A 5E 8E 3B 12 C0 20 44 5C 2A 73
<b>Timestamp</b>	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
<b>Signature Algorithm</b>	SHA-256 ECDSA
<b>Signature</b>	72 bytes: 30 46 02 21 00 E8 15 0D ...
<b>SCT Version</b>	1
<b>Log Operator</b>	Sectigo
<b>Log Key ID</b>	6F 53 76 AC 31 F0 31 19 D8 99 00 A4 51 15 FF 77 15 1C 11 D9 02 C1 00 29 06 8D B2 08 9A 37 D9 13
<b>Timestamp</b>	Thursday, 21 May 2020 at 11:17:51 Central European Summer Time
<b>Signature Algorithm</b>	SHA-256 ECDSA
<b>Signature</b>	71 bytes: 30 45 02 21 00 D9 F5 21 ...
<b>Extension</b>	Certificate Authority Information Access ( 1.3.6.1.5.5.7.1.1 )
<b>Critical</b>	NO
<b>Method #1</b>	CA Issuers ( 1.3.6.1.5.5.7.48.2 )
<b>URI</b>	<a href="http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt">http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt</a>
<b>Method #2</b>	Online Certificate Status Protocol ( 1.3.6.1.5.5.7.48.1 )
<b>URI</b>	<a href="http://GEANT.ocsp.sectigo.com">http://GEANT.ocsp.sectigo.com</a>
<b>Fingerprints</b>	
<b>SHA-256</b>	6C B5 C9 D6 65 CF 7F 87 74 8B 8B D0 84 69 D0 01 C9 41 11 93 F7 FD 7D B5 F2 3A 75 B7 87 E5 28 D0
<b>SHA-1</b>	DF 5E 53 9B CC BB 7F 4F A9 FC EC BD 40 08 D3 C2 C6 78 F7 0C

# Datoteke

- **.CER/.CRT/.DER** – binarni, DER kodirani certifikat (ili niz certifikata)
- **.PEM** – dodatno kodiran po **Base64**
  - počinje retkom “-----BEGIN CERTIFICATE-----”
- **.PFX** – PKCS#12, javni i privatni ključ (zaštićen lozinkom)
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

# Certifikat X.509 - .CRT

```
$ hexdump -C mycert.crt
```

00000000	30	82	05	30	30	82	04	18	a0	03	02	01	02	02	10	08	0..00.....
00000010	a3	71	e3	32	95	57	63	54	96	58	82	75	b3	95	12	30	..q.2.WcT.X.u...0
00000020	0d	06	09	2a	86	48	86	f7	0d	01	01	0b	05	00	30	69	...*H.....0i
00000030	31	0b	30	09	06	03	55	04	06	13	02	4e	4c	31	16	30	1.0....U....NL1.0
00000040	14	06	03	55	04	08	13	0d	4e	6f	6f	72	64	2d	48	6f	...U....Noord-Ho
00000050	6c	6c	61	6e	64	31	12	30	10	06	03	55	04	07	13	09	lland1.0....U....
00000060	41	6d	73	74	65	72	64	61	6d	31	0f	30	0d	06	03	55	Amsterdam1.0....U
00000070	04	0a	13	06	54	45	52	45	4e	41	31	1d	30	1b	06	03	....TERENA1.0...
00000080	55	04	03	13	14	54	45	52	45	4e	41	20	50	65	72	73	U....TERENA Pers
00000090	6f	6e	61	6c	20	43	41	20	33	30	1e	17	0d	31	35	30	onal CA 30...150
000000a0	39	31	37	30	30	30	30	30	30	5a	17	0d	31	38	30	39	91700000Z..1809
000000b0	31	37	31	32	30	30	30	30	5a	30	67	31	0b	30	09	06	17120000Z0g1.0..
000000c0	03	55	04	06	13	02	48	52	31	0f	30	0d	06	03	55	04	..U....HR1.0....U.
000000d0	07	13	06	5a	61	67	72	65	62	31	2e	30	2c	06	03	55	...Zagreb1.0,...U
000000e0	04	0a	13	25	46	61	6b	75	6c	74	65	74	20	65	6c	65	...%Fakultet ele
000000f0	6b	74	72	6f	74	65	68	6e	69	6b	65	20	69	20	72	61	ktrotehnike i ra
00000100	63	75	6e	61	72	73	74	76	61	31	17	30	15	06	03	55	cunarstval.0....U
00000110	04	03	13	0e	4d	69	6c	6a	65	6e	6b	6f	20	4d	69	6b	....Miljenko Mik
00000120	75	63	30	82	01	22	30	0d	06	09	2a	86	48	86	f7	0d	uc0.."0...*H...
	.	.	.														

# Certifikat X.509 - .PEM

```
$ cat mycert.pem
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIIFMDCCBBigAwIBAgIQCKNx4zKVV2NULLiCdbOVEjANBgkqhkiG9w0BAQsFADBp  
MQswCQYDVQQGEwJOTDEWMBQGA1UECBMNTm9vcmQtSG9sbGFuZDESMBAGA1UEBxMJ  
QW1zdGVyZGFtMQ8wDQYDVQQKEwZURVJFTkExHTAbBgNVBAMTFFRFUkVOQSBQZXJz  
b25hbCBDQSAzMb4XDTE1MDkxNzAwMDAwMFoXDTE4MDkxNzEyMDAwMFowZzELMAkG  
A1UEBhMCSFIxDzANBgNVBActB1phZ3J1YjEuMCwGA1UEChMlRmFrdWx0ZXQgZWx1
```

```
...
```

```
tM8DqHDMa6RhNmrxJ1ldokQIVh94RLfQESnm0UHNEXSStDa7nSAcdMasDnH3avvh  
yIeC9dS1H9wT4Hiu7t48vw04jeUgCbbRGmg1Yhg5Dpekj244
```

```
-----END CERTIFICATE-----
```

# Certifikat X.509

(1/3)

```
$ openssl x509 -in mycert.pem -text -noout
```

Certificate:

Data:

    Version: 3 (0x2)

    Serial Number:

        08:a3:71:e3:32:95:57:63:54:96:58:82:75:b3:95:12

    Signature Algorithm: sha256WithRSAEncryption

    Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Personal CA 3

    Validity

        Not Before: Sep 17 00:00:00 2015 GMT

        Not After : Sep 17 12:00:00 2018 GMT

    Subject: C=HR,L=Zagreb,O=Fakultet elektrotehnike i racunarstva,CN=Miljenko Mikuc

    Subject Public Key Info:

        Public Key Algorithm: rsaEncryption

        Public-Key: (2048 bit)

        Modulus:

            00:9d:44:b8:ed:f6:a1:4a:1b:31:dd:8d:aa:d4:a2:

            . . .

# Certifikat X.509

(2/3)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA

X509v3 Subject Key Identifier:

BA:12:55:BC:2B:D4:08:C2:0A:BC:90:E4:B7:C5:75:82:DD:AA:BF:E7

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Alternative Name:

email:miljenko.mikuc@fer.hr

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication, E-mail Protection

X509v3 Certificate Policies:

Policy: 2.16.840.1.114412.4.1.2

CPS: <https://www.digicert.com/CPS>

# Certifikat X.509

(3/3)

X509v3 CRL Distribution Points:

Full Name:

URI:<http://crl3.digicert.com/TERENAPersonalCA3.crl>

Full Name:

URI:<http://crl4.digicert.com/TERENAPersonalCA3.crl>

Authority Information Access:

OCSP - URI:<http://ocsp.digicert.com>

CA Issuers - URI:<http://cacerts.digicert.com/TERENAPersonalCA3.crt>

Signature Algorithm: sha256WithRSAEncryption

04:ce:64:89:c6:f2:5d:ee:dd:67:75:8a:ea:d0:98:41:09:4e:  
a4:f3:1d:27:91:47:18:c9:1f:af:fd:ae:80:8c:e6:14:4d:a4:  
26:29:91:e4:38:5b:8a:52:5d:82:e6:d4:58:7a:b5:4c:a7:bd:  
.  
.  
.  
e6:d1:41:cd:11:74:92:b4:36:bb:9d:20:1c:74:c6:ac:0e:71:  
f7:6a:fb:e1:c8:87:82:f5:d4:b5:1f:dc:13:e0:78:ae:ee:de:  
3c:bf:0d:38:8d:e5:20:09:b6:d1:1a:68:25:62:18:39:0e:97:  
a4:8f:6e:38

# Standardi i preporuke

- ASN.1: Abstract Syntax Notation One (ASN.1)
  - opis struktura podataka koje se mogu serijalizirati na jedinstven način, neovisno o korištenoj platformi
- ITU-T X.690
  - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- BER - Basic Encoding Rules
  - Format kodiranja apstraktnih informacija u tok podataka. Specificira slijed okteta. Sintaksa definira elemente za prikaz osnovnih tipova podataka, strukturu informacija o dužini i način definiranja složenih ili miješanih tipova podataka.
    - CER - Canonical Encoding Rules
    - DER - Distinguished Encoding Rules

# Standardi i preporuke

- DER - Distinguished Encoding Rules
  - osigurava točno jedan način kodiranja ASN.1 vrijednosti
  - namijenjen situacijama kad je potrebno jedinstveno kodiranje
    - npr. u kriptografiji - osigurava da digitalno potpisana podatkovna struktura rezultira jedinstvenim serijaliziranim prikazom
  - kanonski oblik BER
    - npr. BER kodira logičku vrijednost za laž s vrijednošću 0, a vrijednost logičke istine se može prikazati na 255 načina.
    - DER kodira logičke vrijednosti istine i laži na točno jedan način
- CER - Canonical Encoding Rules (CER)
  - razlikuje se od DER u načinu prikaza duljine podataka
  - DER uvijek ima oznaku duljine podataka na početku, a CER koristi oktet za oznaku kraja konteksta
  - CER zahtijeva manje meta podataka za velike kodirane vrijednosti

# Standardi i preporuke

- PKCS - Public-Key Cryptography Standards (RSA Laboratories)
  - PKCS #12 – definira format datoteke za pohranu privatnog X.509 ključa uz javni X.509 certifikat (zaštićene lozinkom temeljenom na simetričnom ključu)
  - PKCS #7 – definira sintaksu šifriranih poruka
    - za potpisivanje ili šifriranje poruka u PKI te za dostavu informacija o certifikatu (kao odgovor na poruku PKCS#10)
    - temelj standardu S/MIME
  - PKCS #10 - definira format poruke koja se šalje CA kao zahtjev za certificiranjem javnog ključa

# Standardi i preporuke

- CMS - Cryptographic Message Syntax
  - IETF-ov standard (RFC 5652) za kriptografski zaštićene poruke
  - može se koristiti za digitalno potpisivanje, sažimanje, autentifikaciju ili šifriranje bilo kojeg oblika digitalnih podataka
  - izveden iz standarda PKCS #7
  - osnovna kriptografska komponenta mnogih standarda
    - npr. S/MIME, PKCS #12 i RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

# Važenje certifikata

- javni ključevi
  - mogu se koristiti kroz dugi vremenski period (desetljeća)
    - zbog provjere potpisa
- privatni ključevi
  - trebaju imati što kraće vrijeme važenja
- opoziv ključa
  - ako je ključ kompromitiran treba ga opozvati
  - ako je ključ opozvan, potpisani dokument ne vrijedi (osim kada ima vremensku oznaku, „timestamp“)
  - ako je ključ opozvan, svi dokumenti koji su njime šifrirani su kompromitirani
- provjera certifikata
  - obavezna! (pošiljatelj / primatelj)
  - treba uključivati provjeru važenja certifikata i provjeru potpisa certifikata
  - ako je potrebno arhivirati potpisani dokument: „timestamp“

# Valjanost certifikata

- Polja u certifikatu: „not valid before” i „not valid after”
- Za vrijeme roka valjanosti certifikat može biti opozvan
  - Gubitak ili kompromitacija privatnog ključa, promjena naziva ili imena, ...
- *Certificate Revocation List (CRL)* – lista opozvanih certifikata
  - CRL je digitalni objekt s rokom valjanosti koji sadrži listu opozvanih certifikata te vrijeme i razlog opoziva (digitalno potpisana od strane CA)
  - u certifikatu su navedene adrese i načini pristupa CRL ([https](https://), [ldap](ldap://))
- **OCSP** - Online Certificate Status Protocol
  - OCSP stapling: poslužitelj, uz certifikat, dostavlja klijentu i vremenski ovjeren rezultat OCSP provjere od strane CA

# Dohvaćanje CRL

- objava CRL
  - u certifikatu piše gdje je CRL
  - Directory Address: CN=CRL58, OU=RDC, O=FINA, C=HR
  - URI:ldap://rdc-ldap.fina.hr/ou=RDC,  
o=FINA,c=HR?certificateRevocationList%3Bbinary
  - URI: <http://rdc.fina.hr/crls/rdc.crl>
  - URI: <http://srl3.digicert.com/TERENAPersonalCA34.crl>
- javni imenik i HTTP
- OCSP - Online Certificate Status Protocol
  - RFC 6960
    - OCSP - URI: <http://ocsp.digicert.com>

# Dohvaćanje CRL

```
$ wget http://crl3.digicert.com/TERENAPersonalCA3.crl  
  
$ openssl crl -inform DER -outform PEM \  
  -in TERENAPersonalCA3.crl -out TERENAPersonalCA3.pem  
  
$ openssl crl -in TERENAPersonalCA3.pem -text -noout  
Certificate Revocation List (CRL):  
...  
Issuer: /C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA Personal CA 3  
Last Update: Oct 27 18:00:22 2015 GMT  
Next Update: Nov 3 17:00:00 2015 GMT  
...  
Revoked Certificates:  
  Serial Number: 0E085BF033E3E00C05454B91CDE4C0ED  
    Revocation Date: Feb 3 12:47:53 2015 GMT  
  . . .  
  Serial Number: 095819C43C84DEA4B14875B765DA18E4  
    Revocation Date: Oct 26 15:04:50 2015 GMT  
  Signature Algorithm: sha256WithRSAEncryption  
    b1:67:df:f6:a3:0f:43:42:cd:cc:af:5e:ae:f1:13:32:53:82:  
  . . .  
  4d:a0:7f:95
```

# Dohvaćanje CRL

```
$ openssl ocsp  \
  -text \
  -issuer TERENA\ Personal\ CA\ 3.pem \
  -cert GordanGledecDigiCertCertifikat.pem \
  -VAfile TERENA\ Personal\ CA\ 3.pem \
  -url http://ocsp.digicert.com
```

# Dohvaćanje CRL

OCSP Response Data:

OCSP Response Status: successful (0x0)  
Response Type: Basic OCSP Response  
Version: 1 (0x0)  
Responder Id: F021E94977739F85AE183BE852701406ED42EECA  
Produced At: Oct 28 09:37:00 2015 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1  
Issuer Name Hash: BD3B9EE18745EFF24C919C59BDECACA670A50828  
Issuer Key Hash: F021E94977739F85AE183BE852701406ED42EECA  
Serial Number: 0E1A6B4B1FC6D9EFD036FD82E7164138

Cert Status: good

This Update: Oct 28 09:37:00 2015 GMT

Next Update: Nov 4 08:52:00 2015 GMT

Signature Algorithm: sha256WithRSAEncryption

ab:d0:fd:d2:81:e2:96:d1:9f:2b:62:5c:fb:e1:56:18:1a:fc:

...

# Korisnici PKI

- organizacije i pojedinci koji koriste PKI
- nositelj certifikata (Certificate holder)
  - subjekt certifikata koji raspolaže s privatnim ključem
    - zahtjeva certifikat od CA kontaktirajući RA
    - dobiva certifikat od CA i koristi ga
    - autentificira se, izrađuje elektronički potpis, dešifrira podatke i sl.
- pouzdajuće strane (Relying parties)
  - korisnici koji raspolažu s javnim ključem
    - identificiraju CA kao početnu točku kojoj vjeruju
    - koriste repozitorij
    - provjeravaju potpis, šifriraju podatke i sl.

# Certifikacijsko tijelo

- Certificate Authority (CA) - povjerljiva treća strana
  - središnji i odgovorni servis sustava PKI
  - izdaje i potpisuje certifikate i jamči vezu subjekta s javnim ključem
  - izdaje CRL i upravlja informacijama o statusu certifikata
  - nužna adekvatna zaštita privatnog ključa certifikacijskog tijela
  - u tehničkom smislu: hardver i softver koji potpisuje certifikate i CRL
  - u tehnološkom smislu: skup ljudi, procedura, standarda i politika
- certifikati svih poznatih izdavatelja ugrađeni su u preglednike ili operacijski sustav (certificate store, keychain,...)
  - unutar organizacije je moguće kreirati i vlastito certifikacijsko tijelo koje izdaje samopotpisani certifikat („self-signed certificate”)

# Odgovornosti CA

- zaštita svog privatnog ključa
- provjera točnosti informacija u certifikatu (prije izdavanja)
- zaštita profila
  - certifikati i CRL se izdaju sukladno svom profilu
- održavanje ažurnosti CRL
- distribuirati (objavljivati) certifikate i CRL
- održavati arhivu za provjeru certifikata i nakon njenog isteka
- moguće je delegiranje odgovornosti trećim stranama
  - registracijsko tijelo („Registration Authority”, RA) - zbog rasprostranjenosti uređa
  - javni imenik - zbog povećanja dostupnosti
  - arhiva - zbog sigurnijeg i dugotrajnijeg čuvanja arhivskih podataka

# Certificate Policy - CP

- u koju svrhu mogu koristiti ovaj certifikat?
- politika, “policy”
  - skup implementiranih procedura
  - primjena: sve komponente PKI - CA, RA, javni imenik
- Certificate Policy (CP)
  - skup pravila koja ukazuju na prikladnost certifikata za određenu zajednicu ili skupinu sa zajedničkim sigurnosnim zahtjevima
  - opisuje pravila rada CA i odgovornosti svih strana
  - javno se objavljuje
- Certification Practice Statements (CPS )
  - detaljno opisuje kako CA implementira CP
  - ne treba biti javno objavljen

# Dodatni servisi

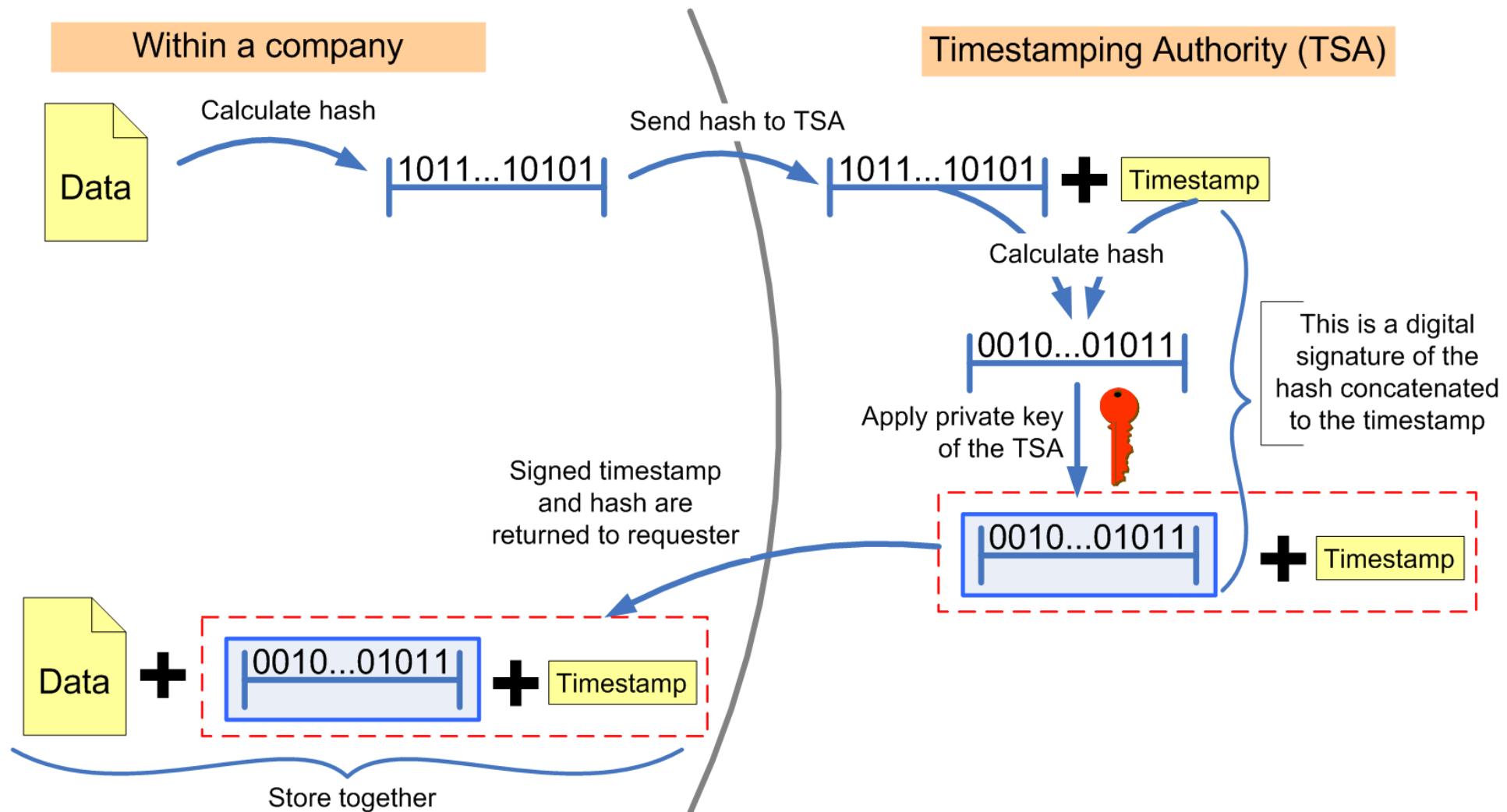
- Timestamp Authority (TSA) - **usluga vremenske ovjere**
  - podatak je postojao u trenutku izrade potpisa
  - certifikat je bio valjan u trenutku izrade potpisa
  - potpis je izrađen prije datuma i vremena TS
  - nužno za izradu kvalificiranog potpisa
  - poslovni modeli
    - besplatne informacije – bez autentifikacije
    - plaćanje po zahtjevu – s autentifikacijom

# Arhitektura TS

- TS (Timestamp) – servis vremenske ovjere
  - NTP server, GPS
  - HSM (Hardware security module) za čuvanje privatnog ključa TS
- tijek:
  - potpisani hash dokumenta se šalje TS poslužitelju u obliku zahtjeva
  - TS poslužitelj vraća odgovor potpisan njegovim certifikatom

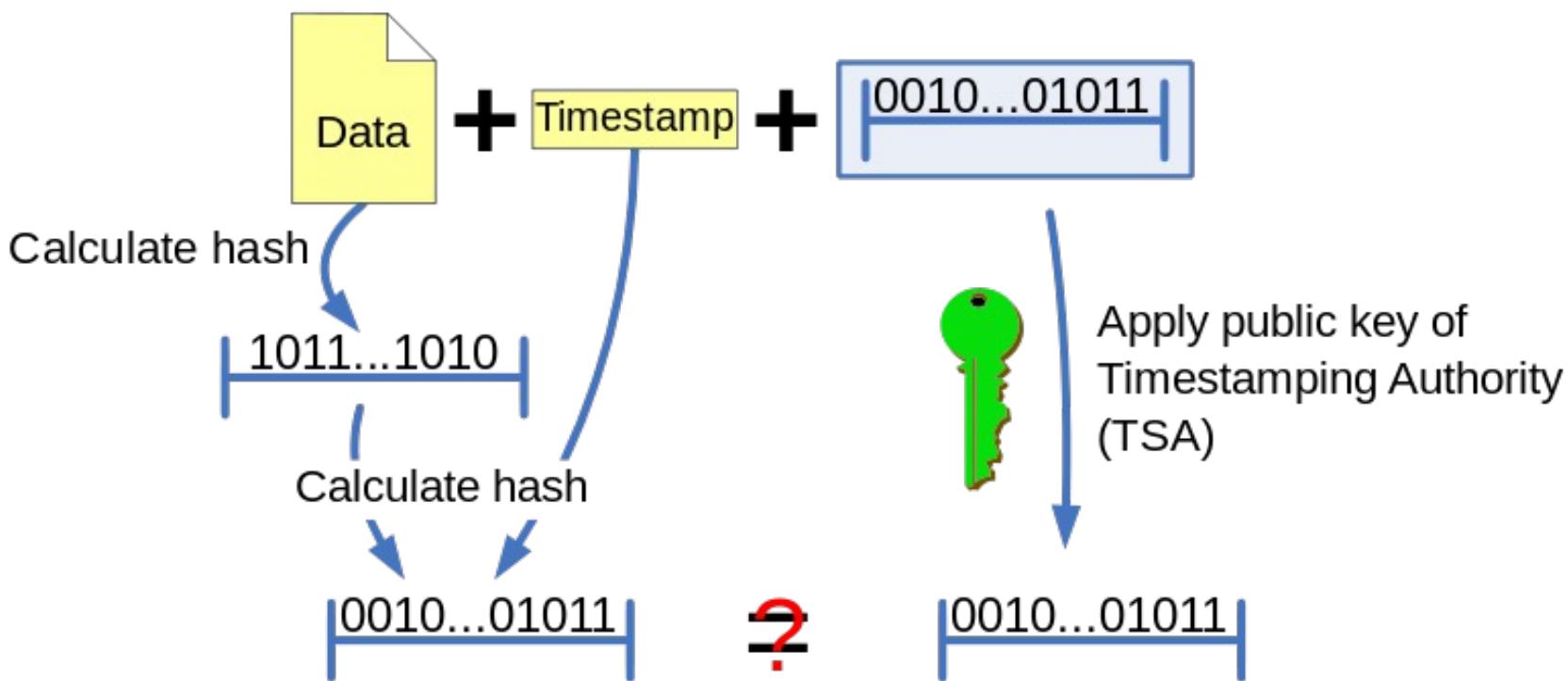
# Arhitektura TS

## Trusted timestamping



# Arhitektura TS

## Checking the trusted timestamp



If the calculated hashcode equals the result of the decrypted signature, neither the document or the timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.

# Problemi sa sustavom PKI

(1)

- certifikacijska tijela su vrlo primamljiv cilj napadačima
  - ima ih mnoštvo koje priznaju proizvođači Web preglednika i ako je bilo koji kompromitiran, cijeli sustav je u opasnosti
  - ne postoji općeprihvaćeni mehanizam provjere koji CA smije izdavati koje certifikate
- primjer velikog napada na CA/incidenta
  - DigiNotar – U rujnu 2011. otkrivena provala u Danski CA te izdavanje lažnih certifikata za Google koji su se koristili za špijuniranje građana Irana. DigiNotar je bankrotirao 2011. godine
- pojedina certifikacijska tijela ne provjeravaju identitet korisnika dobro
- prodaja certifikata s mogućnošću izdavanja certifikata

# Problemi sa sustavom PKI

(2)

- sustav je zbunjujući za prosječnog korisnika Interneta
  - pa čak i za ICT profesionalce
- problemi zbog kojih su korisnici zbunjeni
  - samopotpisani certifikati se ne bi smjeli pojavljivati jer se onda ljudi priučavaju na njih i smatraju ih normalnim/očekivanim
  - Web preglednici variraju način označavanja da se radi o zaštićenoj koneciji čak i između verzija (sa/bez https, različiti lokot)
  - napadači to zloupotrebljavaju tako što lokote stavljuju na razna mesta pokušavajući iskoristiti zbunjenost korisnika
- postojanje različitih vrsta certifikata (Extended/Organization/Domain Validation)
- problem s listama opozvanih certifikata i OCSP-om

# Problemi sa sustavom PKI

(3)

- certifikati koštaju te se izbjegava kupovina
  - pridonosi zbumjenosti korisnika Interneta, Web preglednici sa svojim porukama ne pridonose tome
  - cijena ovisi o trajanju i tipu certifikata
  - Let's Encrypt omogućava besplatne certifikate trajanja cca. 6 mjeseci
- Let's Encrypt
  - temelji se na dokazivanju vlasništva domene izmjenama u DNS-u
  - ako netko preuzme kontrolu nad DNS-om omogućeno je izdavanje lažiranih certifikata
- problem s obnavljanjem certifikata na vrijeme
  - certifikati koji su istekli također zbumuju korisnike
- PKI sustav se smatra nedovoljno dobrim
  - ali boljeg rješenja trenutno nema

# Primjeri izdavatelja certifikata

- elektronička osobna iskaznica, eOI (izdavatelj certifikata: AKD)
  - <http://eid.hr>
- FINA – CA za pravne osobe
  - “Registrar digitalnih certifikata”, <http://rdc.fina.hr/>
- u suradnji s organizacijom GÉANT, CARNET nudi uslugu izdavanja elektroničkih certifikata tvrtke Sectigo Limited
  - OV certifikati (Organization Validation), EV certifikati (Extended Validation),
  - poslužiteljski, klijentski, „document signing”, ...
- poslužiteljski TLS certifikati „Let's Encrypt”
  - <https://letsencrypt.org>
  - DV (Domain Validation)
  - RFC 8555: ACME (Automatic Certificate Management Environment)



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

TLS



# Creative Commons



- **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.

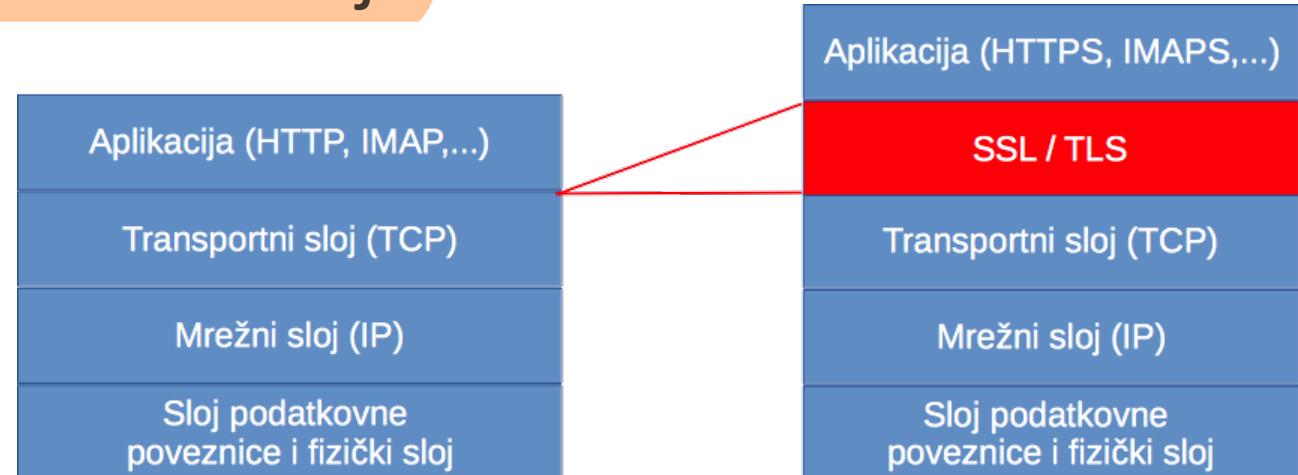


U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci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

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

# Model prijetnje

- Protokol TLS služi za zaštitu komunikacije
- Prepostavke:
  - Krajnje točke komunikacije su sigurne
  - Ostali sustavi mogu biti pod kontrolom napadača
  - Napadač ima potpunu kontrolu nad komunikacijskim kanalom
    - Može proizvoljno mijenjati pakete, ubacivati pakete, duplicirati, ...
  - Eksplicitno ne brinemo o napadima uskraćivanja usluge
    - Napadač presječe komunikacijski kanal, zaustavi komunikaciju, ...
    - Protiv njih se je izuzetno teško nositi s dizajnom protokola



# Protokol TLS

TLS osigurava:

- autentifikaciju poslužitelja (i klijenta)
  - omogućava klijentu provjeru identiteta poslužitelja (certifikat)
  - omogućava poslužitelju provjeru identiteta korisnika (certifikat)
- privatnost podataka
  - nakon dogovora, svi podaci se šalju šifrirano korištenjem dogovorenog tajnog, dijeljenog simetričnog ključa
- cjelovitost (integritet) podataka
  - poruke sadrže MAC, „Message Authentication Code“

# Povijest razvoja protokola SSL i TLS

Protokol	Godina	Opis/Napomena
SSLv1	?	Interno razvijen u tvrtki Netscape Communications. Nikad nije javno objavljen.
SSLv2	1995.	RFC6176 zabranjuje upotrebu ovog protokola zbog niza manjkavosti koje ga čine nesigurnim.
SSLv3	1996.	Više se ne smatra sigurnim. U pripremi je RFC da se njegova upotreba zabrani.
SSL v3.1/TLS 1.0	1. 1999.	Opisan u RFC2246, nije preporučeno korištenje
SSL v3.2/TLS 1.1	4. 2006.	Opisan u RFC4346, nije preporučeno korištenje
TLS 1.2	8. 2008.	Opisan u RFC5246. najčešće korištena verzija
TLS 1.3	8. 2018.	Opisan u RFC8446. Najnovija i trenutno najsigurnija verzija.

# Stanje web poslužitelja

podrška za različite verzije SSL/TLS na web poslužiteljima na Internetu:

- <https://www.ssllabs.com/ssl-pulse/>, siječanj 2022.:
  - SSL v3.0 podržan na 2,8% poslužitelja  
(2020.: 4,2%, 2018.: 8,7%, 2016.: 19,9%, 2015.: 30,0%)
  - TLS v1.0 podržan na 39,3%  
(2020.: 51,5, 2018.: 71,3 %, 2016.: 95,9%, 2015.: 98,8%)
  - TLS v1.1 podržan na 43,0%  
(2020.: 58,5%, 2018.: 79,1%, 2016.: 79,2%, 2015.: 68,4%)
  - TLS v1.2 podržan na 99,6%  
(2020.: 99,0, 2018.: 94,3 %, 2016.: 81,7%, 2015.: 70,7%; 2013.: 15,1%)
  - TLS v1.3 podržan na 51,4% poslužitelja  
(2020: 39,8%, 2018.: 10.5 %)

# Aplikacije koje koriste TLS

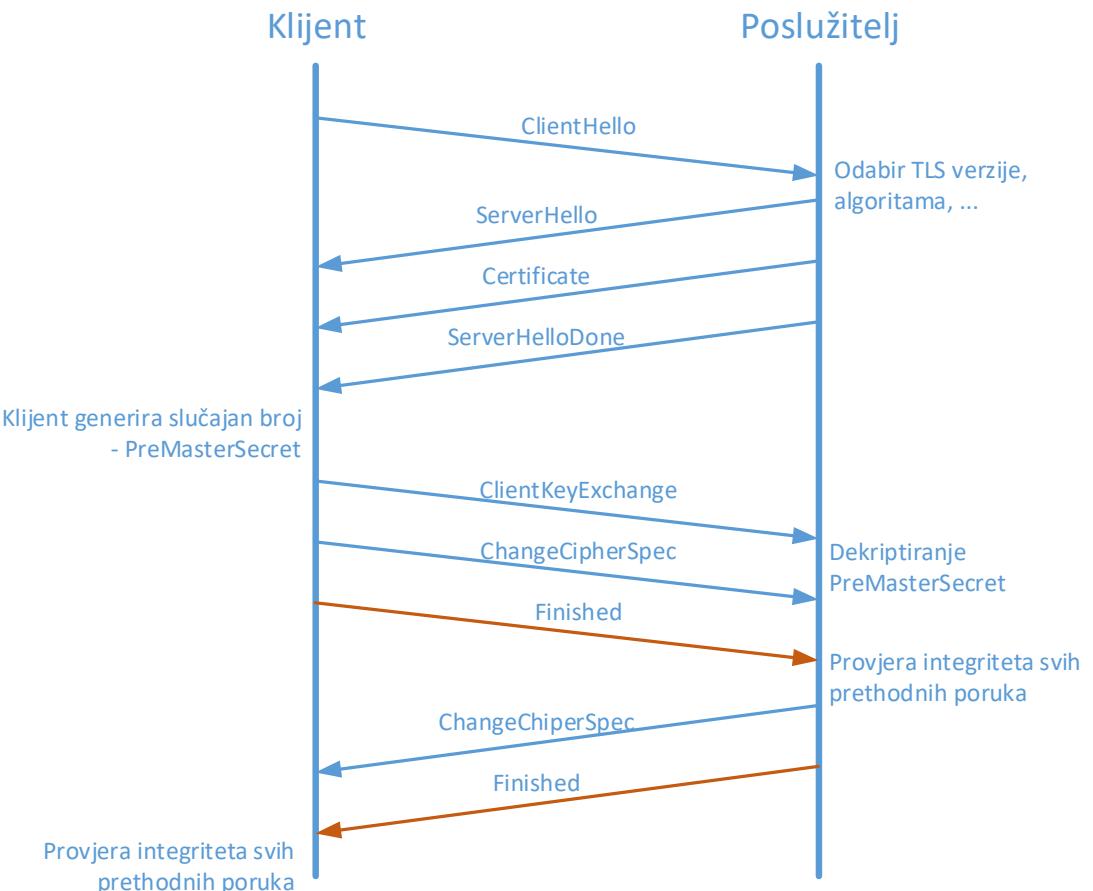
https	443/tcp	# http protocol over TLS/SSL
smtp	25/tcp	# STARTTLS keyword (RFC 2487)
ldaps	636/tcp	# ldap protocol over TLS/SSL (was sldap)
ftps-data	989/tcp	# ftp protocol, data, over TLS/SSL
ftps	990/tcp	# ftp protocol, control, over TLS/SSL
telnets	992/tcp	# telnet protocol over TLS/SSL
imaps	993/tcp	# imap4 protocol over TLS/SSL
imap4	143/tcp	# STARTTLS keyword (RFC 2595)
pop3s	995/tcp	# pop3 protocol over TLS/SSL (was spop3)
pop3	110/tcp	# STLS keyword (RFC 2595)
domain-s	853/tcp	# DNS over TLS [RFC7858]
domain-s	853/udp	# DNS over DTLS [RFC8094]
...		

# HTTP + TLS

- Najčešća upotreba TLS-a: **HTTPS**
  - Korisnik na klijentskoj strani (u pregledniku) zahtjeva dokument s URL koji sadrži **https** umjesto **http**
  - Preglednik prepoznaje SSL/TLS zahtjev i uspostavlja konekciju s poslužiteljem na **TCP portu 443**
  - Klijent inicira „handshake” korištenjem protokola „record” (u ovoj fazi se ne koristi šifriranje i provjera integriteta)

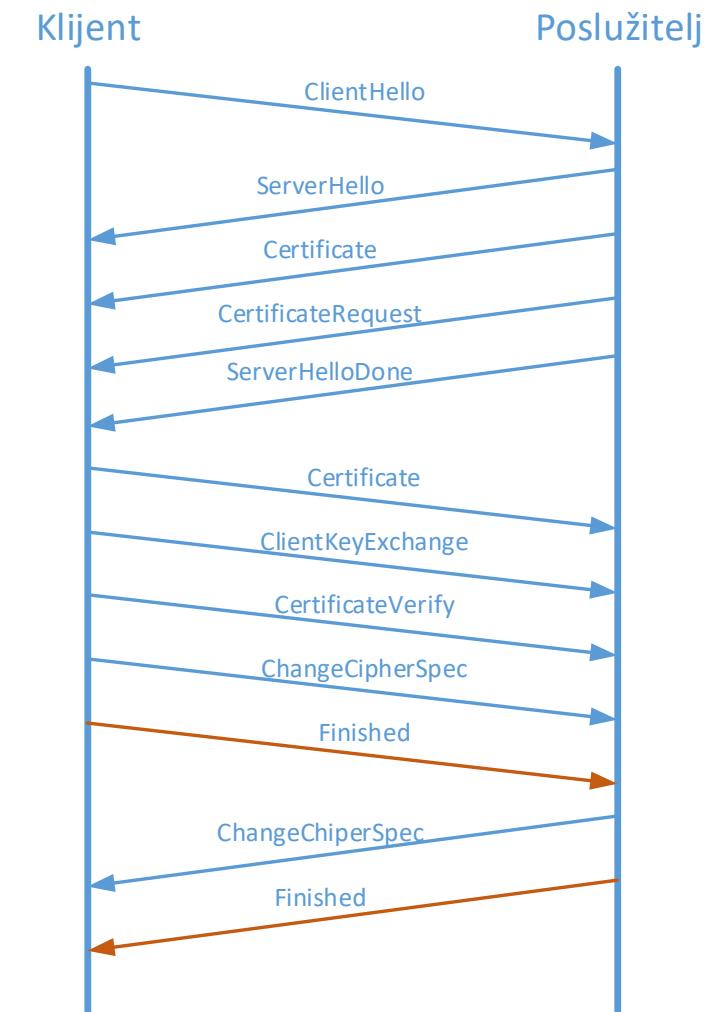
# Osnovna funkcionalnost protokola

- Potvrda identiteta poslužitelja i zaštita tajnosti i autentičnosti komunikacije
- Izvršava se nad protokolom TCP
  - Postoji i varijanta nad protokolom UDP – DTLS (prvenstveno definiran zbog VoIP-a)
    - UDP varijanta je gotovo identična TCP varijanti
- Za one koji žele znati više: „The Illustrated TLS Connection”: <https://tls13.ulfheim.net>



# Autentifikacija klijenta i poslužitelja

- Protokol također omogućava autentifikaciju klijenta korištenjem certifikata (Certifikat sadrži javni ključ)



# Presretanje protokola

- Za tvrtke je kriptirani mrežni promet problematičan
  - Narušavanje politika i pravila korištenja intraneta i Interneta, skidanje zloćudnog koda, eksfiltracija podataka
  - U slučaju presretanja komunikacije zaštićene TLS-om klijenti dobivaju upozorenje (ili uočavaju nezaštićenu komunikaciju)
  - Moguće je kreiranje vlastitog CA i instaliranje na klijentska računala
  - Određeni Web preglednici imaju „pinned certificates“ na temelju čega se može prepoznati presretanje komunikacije

# Napadi na protokol

- „SSL Stripping” – 29. srpanj 2009.
  - MITM napad s ciljem uklanjanja SSL/TLS protokola
  - Jedan način sprečavanja je korištenjem HSTS (RFC6797)
  - Teško „obranjivo” ako klijent prvi puta pristupa usluzi
- BEAST (CVE-2011-3389) – 23. rujan 2011.
  - Iskorištava se predvidivi IV u CBC načinu rada protokola TLS 1.0
  - Omogućava dešifriranje pojedinih dijelova paketa, najbitnije HTTP kolačića
- CRIME - Compression Ratio Info-leak Made Easy (CVE-2012-4929) – 13. rujan 2012.
  - BREACH (CVE-2013-3587) je varijanta CRIME napada
- POODLE (CVE-2014-3566) – 14. listopad 2014.
  - Padding Oracle On Downgraded Legacy Encryption
  - Napad na CBC implementaciju u SSL 3.0

# Promjene u TLS 1.3

- TLS 1.3 je brži i sigurniji protokol od verzije 1.2
  - Uspostavu zaštićene veze moguće je ostvariti u jednom zahtjevu i jednom odgovoru (u TLS 1.2 su potrebne dvije takve razmjene)
    - Skraćuje vrijeme potrebno za prijenos podataka (primjetno i pozitivno)
- Uklonjene su zastarjele i nesigurne komponente protokola
  - SHA-1, RC4, DES, 3DES, DES-CBC, MD5, Arbitrary Diffie-Hellman groups — CVE-2016-0701, EXPORT-strength ciphers – Responsible for FREAK and LogJam

# Implementacije protokola SSL/TLS

- OpenSSL/LibreSSL
- GnuTLS
- BouncyCastle (Android)
- JSSE (Java)
- NSS (Mozilla)
- Schannel (Microsoft)
- Secure Transport (Apple)

# Napadi na implementacije

- Heartbleed (CVE-2014-0160)
  - Propust u OpenSSL implementaciji
  - Neispravno rukovanje „keep-alive” porukom
- Triple Handshake (CVE-2014-1295)
  - Nema provjere da je certifikat tijekom ponovnog pregovaranja (renegotiation) isti kao i prije
  - Apple specifična ranjivost
- FREAK (CVE-2015-0204, CVE-2015-1637, CVE-2015-1067)
  - Propust u nizu implementacija
  - Prsiljava korištenje SSL 3.0 sa slabom kriptografijom te se probijaju ključevi

# Preporuke za korištenje protokola TLS

- RFC 7525: („Best Current Practice“)  
„Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)“
  - update by RFC 8996: „Deprecating TLS 1.0 and TLS 1.1“
- Google: TLS best Practices
- Provjeriti postavke poslužitelja:
  - Testing TLS/SSL encryption  
<https://testssl.sh>

# Preporuke za korištenje protokola TLS

## Privatni ključ:

- 2048-bit RSA ili 256-bit ECDSA
- generirati na povjerljivom računalu uz dovoljnu entropiju
  - neki CA nude uslugu generiranja ključeva – to nije preporučljivo
- ključevi moraju biti zaštićeni lozinkom od početka kako bi se izbjeglo njihovo kompromitiranje kad su pohranjeni na sigurnosnu kopiju
  - u radu, zaštita privatnog ključa lozinkom nije posebno korisna jer se ključ može dohvatiti iz memorije procesa.
- ako je moguće, koristiti HSM (Hardware Security Module), štiti privatni ključ i u slučaju kompromitiranja poslužitelja
- nakon kompromitiranja, stare certifikate je potrebno opozvati i generirati nove ključeve
- certifikate treba redovito obnavljati, jednom godišnje ili češće (ako je moguće automatizirati)
  - kompromitirane certifikate može biti teško opozvati pa je u praksi bolje imati što kraće vrijeme važenja

# Preporuke za korištenje protokola TLS

Pokrivenost domena:

- osigurati dovoljnu pokrivenost naziva domena
  - nazine svih domena za koje će se certifikat koristiti trebaju biti u polju „Subject Alternative Name“ (svi preglednici ne provjeravaju „Common Name“)
- u certifikatu je poželjno imati naziv s www ispred domene i bez www
- „Wildcard“ certifikati se mogu koristiti ali nije dobro omogućiti pristup privatnim ključevima većem broju administratora (s drugih sjedišta)

# Preporuke za korištenje protokola TLS

## Pouzdani CA:

- certifikate treba zatražiti od pouzdanog CA koji prolazi redoviti audit
- izdavanje certifikata mu je važan dio poslovanja
- redovito objavljuje CRL i podržava OCSP
- poželjno je da podržavaju „Extended Validation” (EV)
- koristi jake algoritme za potpis certifikata
  - sigurnost certifikata ovisi o jačini privatnog ključa korištenog za potpisivanje certifikata i jačini funkcije sažimanja korištene za potpis
- koristiti „DNS Certification Authority Authorization” (DNS CAA), standard koji vlasniku domene omogućava ograničavanje CA koji mogu izdati certifikate za tu domenu

# Preporuke za korištenje protokola TLS

## Konfiguracija TLS poslužitelja:

- koristiti potpune lance certifikata – kako bi se izbjegli problemi s neispravnim lancima certifikata najbolje je uključiti sve certifikate
- koristiti sigurne protokole:
  - ne koristiti: SSLv2 ili SSLv3
  - izbjegavati TLS v1.0 i TSLv1.1
  - koristiti TLS v1.2 i v1.3
- prednosti korištenja TLS v1.3:
  - bolje performanse (manje kašnjenje)
  - bolja sigurnost
  - izbačena su nesigurna proširenja poput kompresije

# Preporuke za korištenje protokola TLS

Koristiti sigurne „Cipher Suites“:

- koristiti „cipher suites“ koji podržavaju AEAD (Authenticated Encryption with Associated Data): CHACHA20\_POLY1305, GCM i CCM
- koristiti „cipher suites“ koji podržavaju PFS: ECDHE\_RSA, ECDHE\_ECDSA, DHE\_RSA, DHE\_DSS, CECPQ1 i sve podržano u TLS 1.3
  - Forward secrecy (naziva se još i „perfect forward secrecy“) je svojstvo protokola koje omogućava sigurnu komunikaciju koja ne ovisi o poslužiteljevom privatnom ključu.
  - ako nije podržan „forward secrecy“, privatnim ključem poslužitelja mogu se dekriptirati sve snimljene komunikacije
- slabije enkripcije mogu biti podržane, ali samo za stare klijente koji ne podržavaju ništa bolje
- poslužitelj mora uvijek odabrati najbolji Cipher Suites
  - počevši od SSL v3, klijent dostavlja popis cipher suits koje podržava, a poslužitelj treba odabrati najbolji od ponuđenih (a ne prvi koji je podržan)

# Preporuke za korištenje protokola TLS

## Koristiti jaki „Key Exchange“:

- tipično se koristi klasični ephemeral Diffie-Hellman key exchange (DHE) i verzija s eliptičkim elliptic curve variant, ECDHE
  - „RSA key exchange“ ne osigurava forward secrecy
  - 2015., Logjam attack., napad na DHE: slabiji DH key exchanges (e.g., 768 bits) je moguće lako razbiti a neke dobro poznate 1,024-bit DH groups mogu biti probijene od strane državnih tijela te ako se koristi DHE, treba koristiti najmanje 2,048 bita
- preferirani key exchange je ECDHE (snažan i brz)

## Onemogućiti korištenje kompresije:

- 2012., napad CRIME pokazao je da se TLS kompresija ne može implementirati na siguran način
- 2013., TIME i BREACH, napadi na HTTP kompresiju

# Preporuke za korištenje protokola TLS

Utjecaj TLS-a na performanse :

- latencija mreže je veći problem od kriptografskih operacija na CPU
- TLS „handshake“ počinje nakon uspješno obavljenog TCP „handshake“
  - izbjegavati kreiranje novih konekcija, zadržavati otvorene konekcije
  - koristiti HTTP/2 i QUIC
- koristiti OCSP Stapling
  - proširenje protokola OCSP koje omogućava dostavu informacija o važenju certifikata (da nije opozvan) u okviru TLS „handshake“ procesa, direktno od strane poslužitelja te onda klijent ne treba kontaktirati OCSP poslužitelj čime se ubrzava uspostava sigurne konekcije

# Preporuke za korištenje protokola TLS

## Sigurnost HTTP i aplikacija:

- **kriptirati sve**, uključujući JavaScript datoteke, slike, CSS datoteke
  - implicitno povjerenje uslugama treće strane: JavaScript kod s drugog poslužitelja (zanimljivo napadačima)
  - obavezna kriptirana konekcija (zaštita od MITM)
  - isključiti sve nepotrebne usluge
  - koristiti „Subresource Integrity“ (SRI) (kriptografski sažetak)
- provjeravati **kriptografski integritet** kolačića (smanjiti rizik od MITM)
- koristiti **HSTS**, **HTTP Strict Transport Security**
  - onemogućava bilo kakvu nesigurnu konekciju s web sjedištem, automatski pretvara linkove u sigurne i onemogućava „click-through certificate warnings“ (koji su u pravilu pokazatelj aktivnog MITM napada)
- koristiti **CSP**, Content Security Policy, mehanizam kojim se ograničava dohvaćanje „third-party“ sadržaja na nesiguran način (tu ne pomaže HSTS)
- TLS osigurava povjerljivost i integritet komunikacije između korisnika i poslužitelja ali postoje i brojne druge ranjivosti!



SVEUČILIŠTE U ZAGREBU



Diplomski studij

Ak. godina 2022./2023.

# Sigurnost komunikacija

Napadi na DNS

Napadi na protokole usmjeravanja



# Creative Commons



- **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.



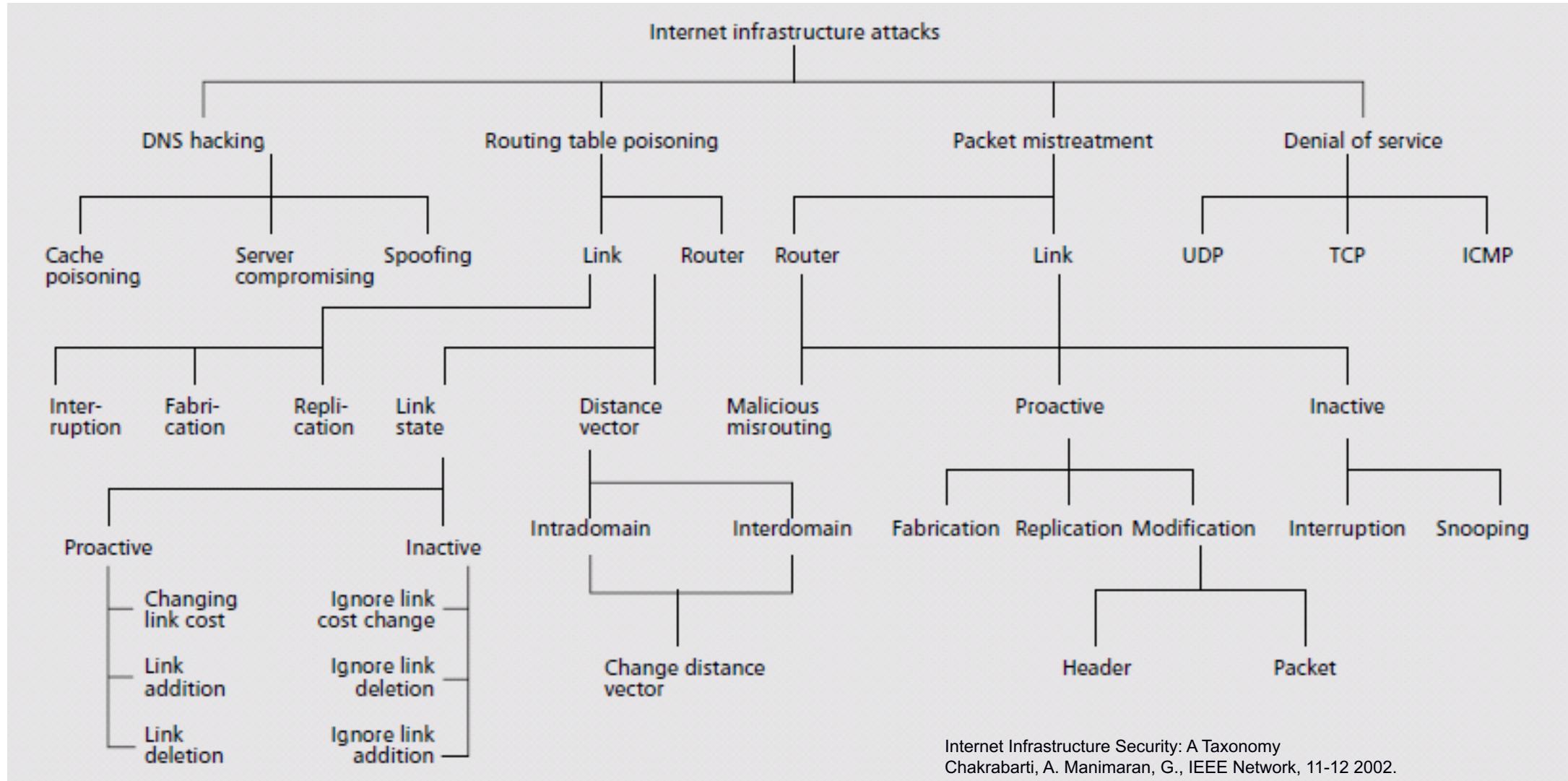
U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci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

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

# Sadržaj

- DNS
- BGP

# Tipovi napada na infrastrukturu Interneta



# Osnovno o sustavu domenskih imena

- raspodijeljeni hijerarhijski sustav i pripadajući protokol razvijen početkom 1980-tih za pretvorbu simboličkih imena u IP adrese
  - od nastanka pa do danas značajno proširen te se radi o raspodijeljenoj hijerarhijskoj bazi ključ-vrijednost
  - vrlo kompleksan sustav koji podržava internacionalna imena
  - ključevi se nazivaju „zаписи ресурса“ (RR, *resource records*)
- usluge sustava upotrebljavaju aplikacije, ne direktno korisnici
- kada ne radi, korisnici kažu kako „Internet ne radi“!

# Primjer DNS upita i odgovora

```
% dig @8.8.8.8 www.amazon.com

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5141
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.amazon.com.           IN      A

;; ANSWER SECTION:
www.amazon.com.          45 IN    CNAME   tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com. 48 IN    CNAME   www.amazon.com.edgekey.net.
www.amazon.com.edgekey.net. 18425 IN   CNAME   e15316.a.akamaiedge.net.
e15316.a.akamaiedge.net. 20 IN    A        23.47.213.240
```

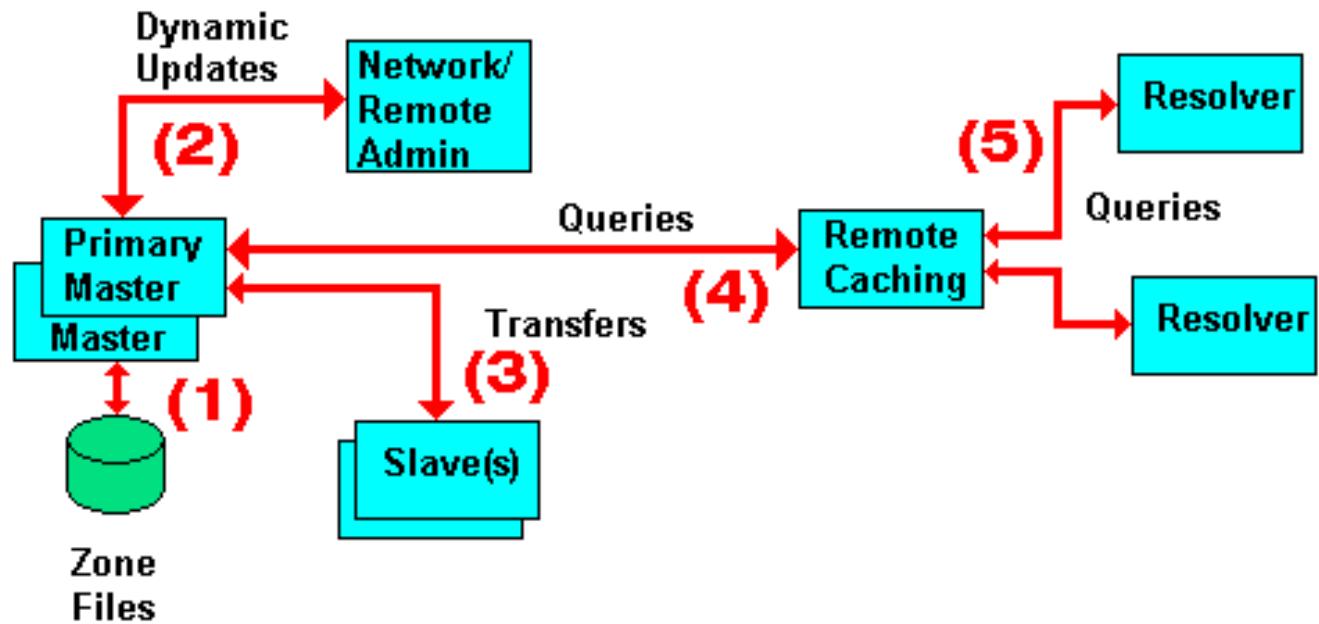
# Osnovno o sustavu domenskih imena

- generičke komponente sustava su
  - klijent, „resolver”, autoritativni poslužitelj, poslužitelj s priručnom memorijom
- u sustavu DNS fiksirani su samo korijenski poslužitelji (engl. root servers)
  - svako računalo dolazi s popisom IP adresa tih poslužitelja
  - svi ostali poslužitelji se dinamički otkrivaju ovisno o potrebi
- svaki poslužitelj može pružati usluge
  - potpuno razrješavanje upita (engl. recursive) – poslužitelji na lokalnim mrežama kojima pristupaju računala spojena na lokalnu mrežu
  - odgovara samo na upite za svoju domenu

# Svrha napada na sustav DNS

- **Sprečavanje pristup određenoj usluzi**
  - Primjerice, slanje negativnih odgovora (kao da DNS naziv ne postoji)
  - Preusmjeravanje zahtjeva na poslužitelj koji ne sadrži traženu uslugu ili ne postoji
- **MITM napad ili podmetanje lažnih sjedišta**
  - Preusmjeravanja komunikacije te potom prosljeđivanje pravom odredištu
  - Varijacija napada je prorušavanje (predstavljanje) kao pravi poslužitelj
  - Ranjivi su Web poslužitelji i poslužitelji elektroničke pošte, ali i drugi poslužitelji
- **Preuzimanje domena**
  - Kompromitiranjem nesigurnih mehanizama osvježavanja preuzima se domena

# Napadi na DNS – točke ranjivosti



1. pokvareni podaci
2. neautorizirana osvježenja
3. promijenjeni podaci o zoni
4. zagađenje *cachea*
5. glumljenje *cachea*
6. glumljenje „mastera“

Trovanje priručne memorije (*cache poisoning*)

<https://spectrum.ieee.org/fresh-phish>

<http://beezari.livejournal.com/141796.html>

# Prijetnje sustavu DNS (1)

- Presretanje paketa
  - Napadač izvršava MITM napad te presreće kompletну komunikaciju
  - Praćenje upita i slanje lažiranih odgovora koji stižu prije legitimnih
  - Napadaču olakšava napad činjenica da se odgovor sastoji od samo jednog UDP paketa
  - Napadač ne mora falsificirati ili na neki drugi način utjecati na sam odgovor, može podmetati i lažne informacije u drugim dijelovima poruke
- Primjena IPsec/TLS i sličnih rješenja nije odgovarajuća
  - Štiti samo pojedine korake, ne s kraja na kraj
  - Zahtjeva uspostavu povjerenja između svih strana
  - Za opterećene poslužitelje značajno podiže opterećenje

# Prijetnje sustavu DNS (2)

- Pogađanje ID vrijednosti i predviđanje upita
  - engl. ID Guessing and Query Prediction
  - Napadač nije na putu i mora pogoditi ID u paketu te izvorišni pristup
    - U određenim situacijama izvorišni pristup je fiksiran na 53
    - Broj pokušaja je  $2^{32}$ , odnosno  $2^{16}$
    - Naravno da napadač mora znati QNAME i QTYPE
  - Napadač može koristiti i dodatne informacije kako bi smanjio broj pokušaja
    - Primjerice, predvidivo generiranje ID-jeva i pristupa
- Zaštita
  - Isti komentari kao i za presretanje paketa

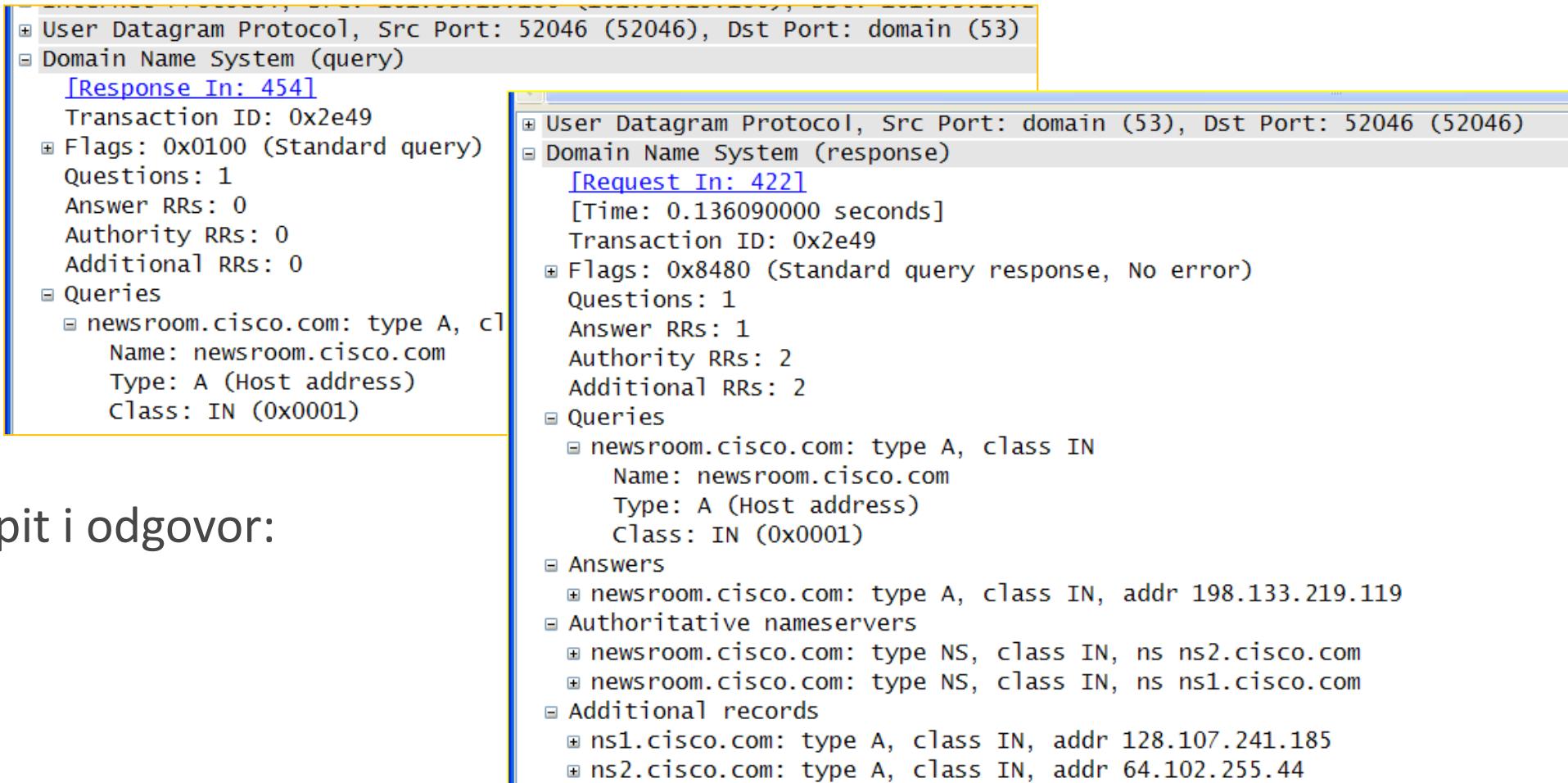
# Prijetnje sustavu DNS (3)

- „Name chaining”?
  - Podskup napada trovanja priručne memorije (engl. cache poisoning)
  - U odgovoru se šalje informacija koja uzrokuje da žrtva šalje DNS upit prema napadačevom poslužitelju
  - U priručni spremnik može se ubaciti informacija koja nije direktno tražena od strane žrtve, ali će ju onda žrtva koristiti
- Zaštita
  - Djelomična zaštita sprečavanja trovanja priručne memorije je provjera relevantnosti dobivenih informacija s obzirom na poslani upit
    - Napad povezivanja imena se ne može tako spriječiti!

# Prijetnje sustavu DNS (4)

- Manipulacija upotrebom poslužiteljima
  - engl. Betrayal By Trusted Server
  - Klijent vjeruje nekom poslužitelju koji je pod kontrolom napadača ili se jednostavno ne ponaša u skladu s očekivanjima
  - Ne mora nužno biti autoritativni poslužitelj
- Uskraćivanje usluge
  - Oko ove prijetnje nije moguće napraviti puno dizajnom protokola (kao u slučaju TLS-a)
  - Rješava se višestrukim DNS poslužiteljima po domeni razmještenima u različitim mrežama
  - Ponekad (pogotovo u slučaju korijenskih poslužitelja) rješava se upotrebom ANYCAST adresa

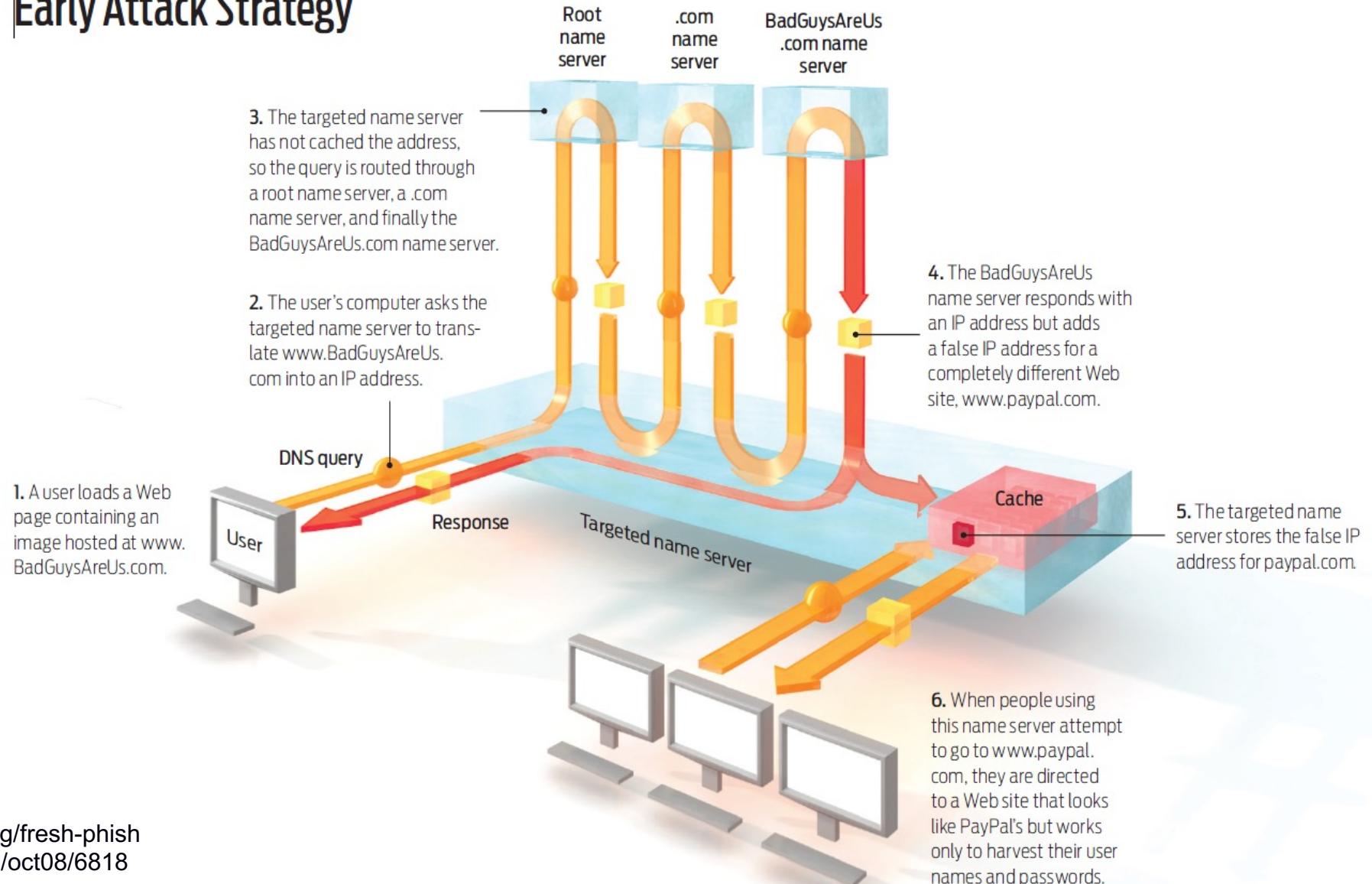
# Primjer napada: „DNS Cache poisoning”



- DNS upit i odgovor:

# DNS Cache poisoning

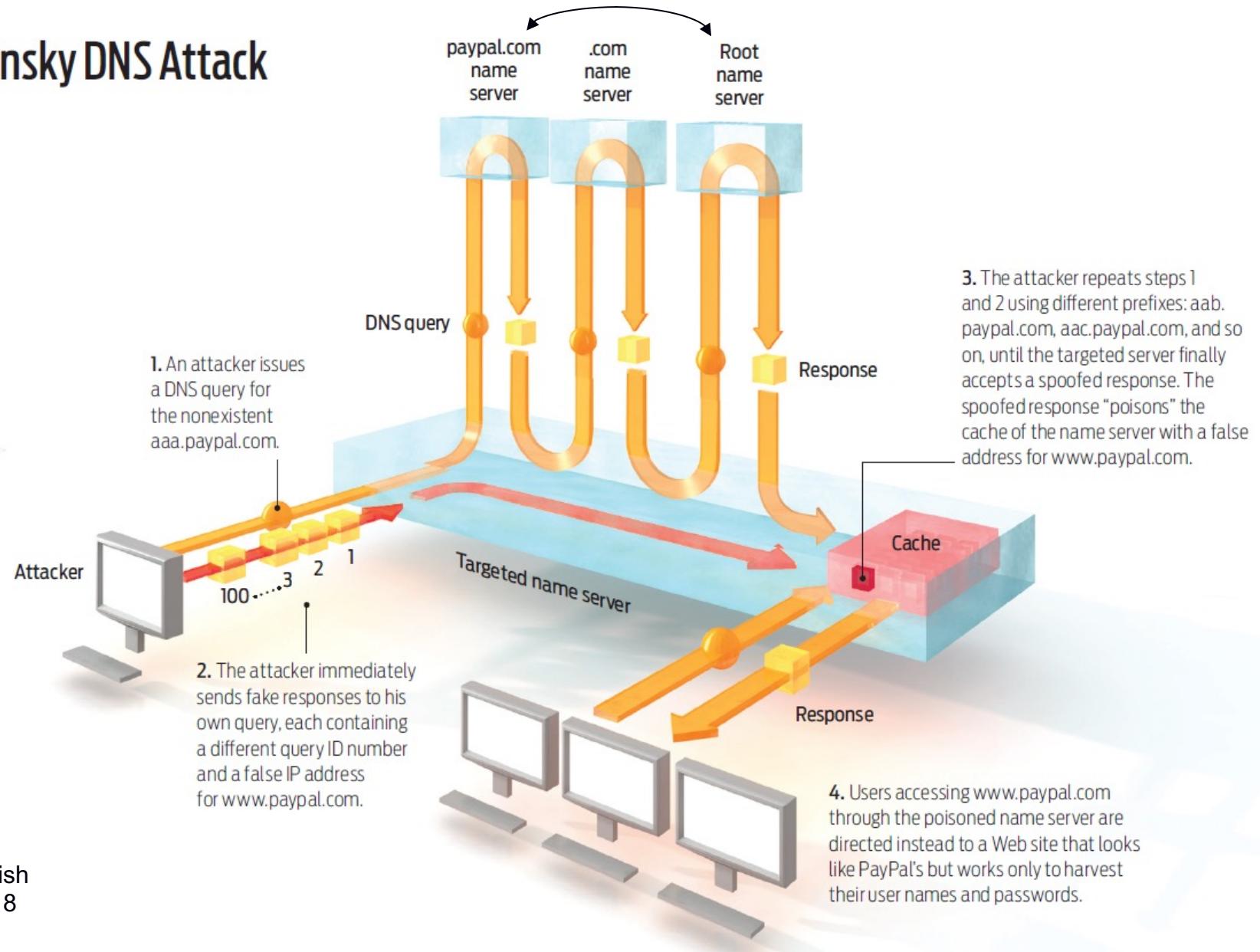
## Early Attack Strategy



Kopirano iz:  
<https://spectrum.ieee.org/fresh-phish>  
<http://spectrum.ieee.org/oct08/6818>

# DNS Cache poisoning

## Kaminsky DNS Attack



Kopirano iz:  
<https://spectrum.ieee.org/fresh-phish>  
<http://spectrum.ieee.org/oct08/6818>

# Zaštita sustava DNS

- TSIG- Transaction Signature
  - provjerava identitet pomoću dijeljenog ključa
  - koristi se kod prijenosa zone ili dinamičkog osvježavanja podataka (između primarnog i sekundarnog poslužitelja)
  - obje strane moraju imati ključ
- specifične zaštite od DNS Cache Poisoning
  - TXID (16 bita) + „random source port“ (16 bita)
- DNSSEC
  - Domain Name System Security Extensions

# Zaštita od DNS Cache Poisoning?

- Napad na DNS „forwarder” (dnsmasq): DNSpooq
  - <https://www.jsof-tech.com/wp-content/uploads/2021/01/DNSpooq-Technical-WP.pdf>
  - koristi se „random port” ali 1 od 64 i uz to napadač mora pogoditi jedan, bilo koji od tih 64 porta: umjesto  $2^{32}$  kombinacija  $2^{32}/64=2^{26}$
  - interno se upiti prikazuju u zapisu „forward record” i napadač treba pogoditi TXID i podatke u odgovarajućem "forward record"
  - ne pamti se cijeli „forward record” već samo „hash” i to prilagođena verzija CRC32 (nije kriptografski sažetak, jednostavno ga je generirati)
  - dnsmasq dozvoljava višestruke zahtjeve s istim nazivom te prihvaca ispravan odgovor na bilo koji od njih
  - potrebno je  $\sim 2^{19}$  upita za uspješan cache poisoning
  - ...

# Zaštita od DNS Cache Poisoning?

- „Side channel attacks”
  - SADDNS: „DNS cache poisoning, the Internet attack from 2008, is back from the dead”
    - <https://arstechnica.com/information-technology/2020/11/researchers-find-way-to-revive-kaminskys-2008-dns-cache-poisoning-attack/>
  - „DNS Cache Poisoning Attack: Resurrections with Side Channels”, ACM CCS 2021
    - [https://www.cs.ucr.edu/~zhiyunq/pub/ccs21\\_dns\\_poisoning.pdf](https://www.cs.ucr.edu/~zhiyunq/pub/ccs21_dns_poisoning.pdf)
    - „Linux has a serious security problem that once again enables DNS cache poisoning”:  
<https://arstechnica.com/gadgets/2021/11/dan-kaminskys-dns-cache-poisoning-attack-is-back-from-the-dead-again/>

# Zaštita sustava DNS: DNSSEC (1)

- engl. Domain Name System Security Extensions
- Osigurava kriptografski dokaz ispravnosti primljenih podataka
- DNSSEC ne osigurava
  - Dinamičko osvježavanje podataka na glavnom DNS poslužitelju (engl. master)
  - Prijenos podataka o zoni (master → slave)
- Klijenti korištenjem resolvera koji provjeravaju valjanost dobivaju zajamčeno sigurne podatke
  - Za podatke koje ne može provjeriti resolver vraća SERVFAIL

# Zaštita sustava DNS: DNSSEC (2)

- Za zaštitu se koristi asimetrična kriptografija
- Podaci, zapisi na poslužitelju (RR – Resource Records), potpisuju se privatnim ključem
  - Javni ključ se objavljuje putem DNS-a i koristi se za provjeru valjanosti potpisa
- Potpisom se osigurava valjanost zapisa s kraja na kraj – između autoritativnog poslužitelja i resolvera
  - Valjanost podataka znači autentičnost izvora podataka i integritet
  - Autentičnost negiranja postojanja zapisa (NXDOMAIN)
- Možemo li tim podacima vjerovati?
  - Da ako je root (“.”) potpisani!

# Zaštita sustava DNS: DNSSEC (3)

- Novi zapisi za podršku DNSSEC [RFC 4034]
  - Resource Record Signature (RRSIG)
  - DNS Public Key (DNSKEY)
  - Delegation Signer (DS)
  - Next Secure (NSEC)
- Nove zastavice u zaglavlju DNS paketa:
  - Checking Disabled (CD), Authenticated Data (AD)
  - Nužna podrška EDNS0 (Extension Mechanisms for DNS)
- Novi bitovi u zaglavlju (temeljeni na EDNS0):
  - DNSSEC OK (DO) – resolver je spremam primiti DNSSEC RR

# Primjer

```
% dig -t any . @a.root-servers.net
;; Truncated, retrying in TCP mode.

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53395
;; flags: qr aa rd; QUERY: 1, ANSWER: 22, AUTHORITY: 0, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.

;.. IN ANY

;; ANSWER SECTION:
. 86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2022040402 1800 900
604800 86400
. 86400 IN RRSIG SOA 8 0 86400 20220417170000 20220404160000 47671 .
jxhEctLYokMAZeUYB1F3KFn1ZQJmdBgWK611UwJW1cCdZ+6XyCxznOdp TQDIyfUX6T84cbVI05KgSq70+Zxm3mZuUKZPNUb5NFmoD9RnfJaHH4cX
19EHsdayTvAwbSvnqh6YKJDk5bp3ZkFv+7J8UBOPv4Cds163/iKGiply dOP3zNa4JRbSxiIz20UoLRN1uhGk/33rZdM/Lfk2IrgT6Nb9lu+xlrqe
Ty/5dnpxwtZ/TCdKf9cFdD/s/jTNtoZxrVfpqh518soQ7C7JFxe+xEG8 zVLjmW751y+QR46YtOK+5oUvb0419p256oQmlzK39iJ/TxRF9biygFuY
vO4pzA==
```

# Problemi sustava DNSSEC

- DNSSEC ne osigurava povjerljivost podataka
  - To je namjerna odluka donesena na početku razvoja protokola
- DNSSEC ne štiti od DDoS napada
- Utjecaj na mrežu i vatrozide
  - Očekuju se puno duži odgovori (do 2KB)
  - Vatrozid ne smije mijenjati DNS odgovore – potpis neće odgovarati
- Vrijeme života digitalnog potpisa
- Kod svake promjene podataka zonu treba ponovo potpisati
- Ključeve treba povremeno mijenjati – više posla!

...

- Napad na DNS „forwarder” (dnsmasq): DNSpooq
  - Bug u implementaciji: ako se koristi DNSSEC, ranjivost tipa „buffer overflow” kod provjere valjanosti odgovora!

# DDoS

- otvoreni rekurzivni poslužitelji
  - "Open Resolver Project" (27.10.2013.): 32 milijuna resolvera koji odgovaraju na upit; 28 milijuna ih predstavlja značajnu prijetnju
- DrDoS - Distributed Reflection DoS attack
  - kombinacija "reflection and amplification": napadač šalje "spoofane" upite "open resolverima" koji vraćaju "pojačani" odgovor (DDoS)
  - upit: 44 okteta, odgovor 4077 okteta
- State of the Internet – Security Report
  - "akamai's [state of the internet] / security, Q3 2014" <http://www.stateoftheinternet.com/resources-web-security-2014-q3-internet-security-report.html>
  - 321 Gbit/s
  - 16 napada >100 Gbit/s

# Neke druge (zlo)upotrebe DNS-a

- DNS sve više služi za raspodijelu sigurnosno osjetljivih podataka
  - Distribucija javnih SSH ključeva poslužitelja
  - Osiguravanje elektroničke pošte
  - Podaci o autentifikacijskom sustavima u tvrtkama
- Autorizacija i autentifikacija na temelju imena domene
  - Napadač može lažirati upite za reverznim razrješavanjem
- Napadači zloupotrebljavaju DNS
  - Eksfiltracija podataka iz tvrtke
  - Upravljanje zaraženim računalima (botovima)
    - Zato se DNS koristi za detekciju zaraženih računala u unutarnjoj mreži (pristup „neobičnim“ domenama)

# Neke druge (zlo)upotrebe DNS-a

- tuneliranje kroz DNS
  - DNS se koristi kao skriveni komunikacijski kanal (kako bi se zaobišao vatrozid)
  - tunelira se SSH, HTTP, bilo kakav TCP
  - koristi se za slanje ukradenih podataka iz mreže
  - koristi se i za zaobilaženje "captive portala" kako bi se izbjeglo plaćanje Wi-Fi usluga

# “DNS over TLS” / “DNS over HTTPS”

- Problem privatnosti, skrivanje meta-podataka
- DNS over HTTPS
  - RFC 8484: "DNS Queries over HTTPS (DoH)"
  - HTTPS i HTTP/2, port 443 (DNS promet "skriven" unutar ostalog šifriranog prometa)
- DNS over TLS
  - RFC 7858: "Specification for DNS over Transport Layer Security"
  - RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS"
  - TCP + TLS, port 853
- Cloudflare DNS resolver: 1.1.1.1 i 1.0.0.1 podržava oba standarda
  - <https://blog.cloudflare.com/dns-resolver-1-1-1-1/>

# Napadi na usmjeravanje

- protokoli za usmjeravanje „drže mrežu na okupu“
  - temeljna zadaća je razmjena informacija „gdje se što nalazi“
- podjela usmjerničkih protokola prema mjestu korištenja:
  - unutar autonomnih sustava (unutarnje usmjeravanje): OSPF, IS-IS, RIP
  - između autonomnih sustava: BGP
- podjela usmjerničkih protokola prema načinu rada:
  - protokoli vektora udaljenosti (engl. *distance vector*)
  - protokoli stanja veze (engl. *link state*)
- napadi se svode na manipulaciju usmjerničkim informacijama kako bi se preusmjeravao promet prema potrebama napadača
  - moguć napad na usmjernike kako bi se ovladalo s njima
  - zaštita vanjskog usmjeravanja je puno teža od zaštite unutarnjeg usmjeravanja
  - izolacija usmjerničkih podataka od korisničkih podataka

# Napadi na usmjeravanje

utjecaj:

- podoptimalno usmjeravanje - može utjecati na aplikacije koje prenose podatke u stvarnom vremenu
- zagušenje - umjetno stvoreno zagušenje uzrokovano preusmjeravanjem prometa na određeni dio mreže
- particioniranje - kreiranje umjetnih particija mreže – nemogućnost komuniciranja s računalima u drugim particijama
- preplavljivanje poslužitelja - trovanje tablica usmjeravanja može se koristiti kao oružje za DoS napade – ruter šalje „update“ poruke koje rezultiraju koncentriranjem paketa na jedan ili više odabralih poslužitelja
- *looping* - kreiranje petlji
- pristup podacima - preusmjeravanje prometa radi snimanja (ilegalni pristup podacima)

# Tipovi napada

- ovise o načinu rada protokola
- “link state protocol” (na primjer OSPF)
  - svaki čvor periodički preplavljuje mrežu stanjima svojih linkova – LSA, “link state advertisement”
  - svaki usmjeritelj izračunava stablo najkraćih putova – SPT, “shortest path tree”
- “distance vector protocols” (na primjer RIP)
  - svaki čvor šalje svoje udaljenosti do svih poznatih mreža svim svojim susjedima
  - po primitku poruke usmjeritelj po potrebi osvježava tablicu usmjeravanja
  - usmjeritelj nema potpune informacije o topologiji mreže

# Tipovi napada

- napadi na link
  - jednaki za oba tipa protokola
  - presretanje
    - potvrde; mogući nesinkronizirani podaci, petlje, DoS
  - ometanje, modificiranje poruka (i generiranje lažnih poruka)
    - digitalni potpisi – povećava sa veličina paketa
    - prihvatljivo kod “link state” / “update” poruka
    - zahtjeva postojanje PKI
  - ponavljanje starih poruka
    - korištenje rednih brojeva i oznaka vremena (timestamp)
- napadi na usmjeritelj
  - nakon toga šalje lažne poruke, ne šalje poruke, ...

# Vanjsko usmjeravanje: BGP

- BGP - Border Gateway Protocol
  - protokol za razmjenu informacija o usmjeravanju između mreža
  - „exterior gateway protocol”
  - RFC 4271: „A Border Gateway Protocol 4 (BGP-4)“
    - Updated by: 6286, 6608, 6793, 7606, 7607, 7705, 8212, 8654
  - dva BGP usmjernika komuniciraju upotrebom TCP veze
  - dva BGP usmjernika razmjenjuju popis mreža za koje znaju te na temelju toga određuju što je na Internetu dostupno i kako se do toga dolazi

# Path Vector Protocol

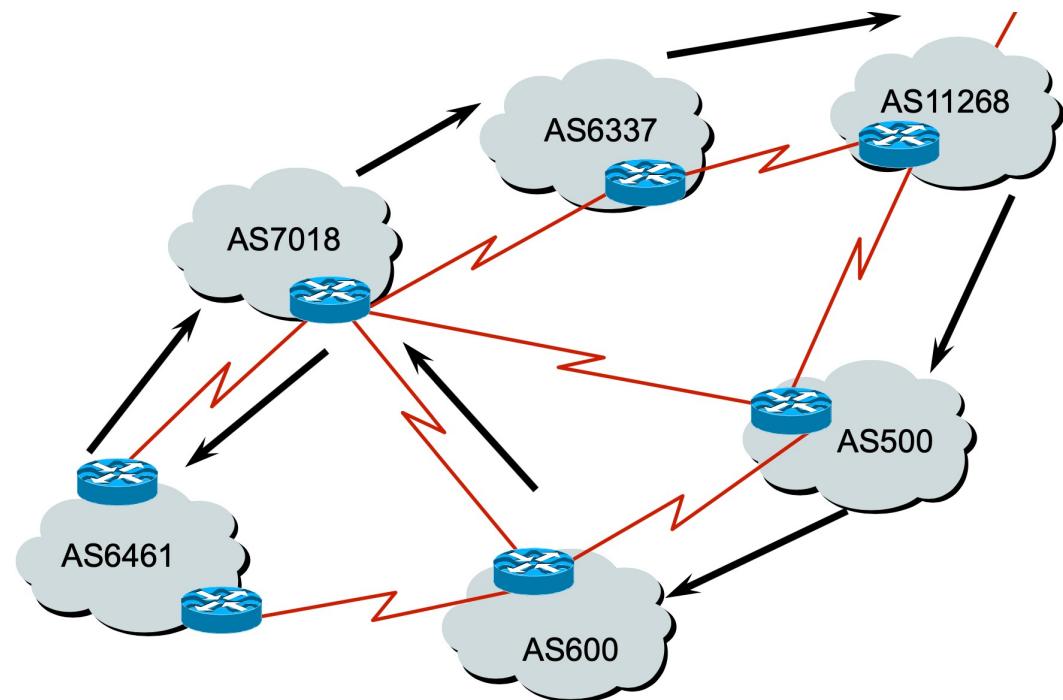
- BGP se klasificira kao „path vector” protokol usmjeravanja

- ruta je zapis odredišta i puta do tog odredišta

- vektor puta se sastoji od slijeda oznaka autonomnih sustava

12.6.126.0/24 207.126.96.43 1021 0 6461 7018 6337 11268

- „AS path”: 6461 7018 6337 11268



# Autonomni sustav

- Autonomous System, AS, je skup povezanih mreža pod kontrolom jednog ili više mrežnih operatora u ime jedne administrativne jedinice ili domene koji na internetu predstavlja zajedničku, jasno definiranu politiku usmjeravanja.
  - unutar autonomnog sustava se koristi ista politika usmjeravanja
  - jedinstveni protokol usmjeravanja
  - u pravilu u vlasništvu i pod kontrolom jedne organizacije
  - identificira se jedinstvenim 32-bitnim cijelim brojem: ASN
  - RFC 5396 definira „asplain” kao standardni način prikaza 32-bitnog ASN (postoji i „asdotted”)
  - u protokolu BGP se koristi za jedinstvenu identifikaciju mreža
  - na Internetu je > 100000 AS-ova
  - svi AS-ovi su ravnopravni!

# Autonomni sustav

- primjeri oznaka autonomnih sustava
  - <http://www.iana.org/assignments/as-numbers>
    - CARNET: AS2108
    - Ericsson Nikola Tesla d.d.: AS209434
  - samo po jedan prefiks oglašava 24 341 AS
  - najviše oglašenih prefiksa od jednog AS je 7003 (AS47331: TTNET, TR)
  - ukupno oglašavanih prefiksa: 834 320

# Napadi na protokol BGP

- informacije koje BGP usmjernici razmjenjuju nisu autentificirane
  - postoji protokol ali se ne koristi – rezultat je da svatko može reći što želi
- koristi TCP
  - problemi protokola TCP: DoS SYN paketima, predviđanje slijednih brojeva (u pravilu riješeno), ...
- prijetnje mogu doći od BGP *speakera* ili od uspostavljene BGP veze
  - može biti ugrožen (iskorištavanjem softverskih nedostataka), krivo konfiguriran (namjerno ili slučajno), ili neautoriziran (iskorištavanjem povredivosti autentifikacije BGP *peera*)
  - **otimanje IP adresa AS-ova**
  - **preusmjeravanja prometa**
- napadi na **poruke**
  - modifikacija, **umetanje, brisanje, ponavljanje ...**
  - krivotvorene (engl. falsification): modifikacije + umetanje

# Sigurnosni ciljevi

- autentifikacija porijekla podataka
  - AS Number Authentication – autentifikacija broja AS-a
    - entitet koji koristi AS-a je autorizirani predstavnik AS-a
  - BGP Speaker Authentication – autentifikacija BGP speakera
    - BGP speaker je autoriziran od strane AS-a
- integritet podataka
  - poruka nije bila nedozvoljeno mijenjana na putu do odredišta
- ispravnost poruka
  - Prefix Origination Verification – verifikacija porijekla prefiksa
    - AS regularno objavljuje prefikse
  - AS Path Verification – verifikacija puta AS-a

# BGP problemi

- "Some people are surprised when networks fail and melt down, but others are surprised when they don't"
  - Sam Halabi, "Internet Routing Architectures"
- "Understanding How Facebook Disappeared from the Internet"
  - <https://blog.cloudflare.com/october-2021-facebook-outage/>
- SuproNet, Češka, 2009.
  - <http://research.dyn.com/2009/02/the-flap-heard-around-the-world/>
- Google DNS briefly hijacked to Venezuela, 2014.
  - <http://arstechnica.com/information-technology/2014/03/google-dns-briefly-hijacked-to-venezuela>
- Repeated attacks hijack huge chunks of Internet traffic, researchers warn, 2013.
  - <http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/>

# BGP problemi

- How an Indonesian ISP took down the mighty Google for 30 minutes (2012)
  - <http://arstechnica.com/information-technology/2012/11/how-an-indonesian-isp-took-down-the-mighty-google-for-30-minutes/>
- Insecure routing redirects YouTube to Pakistan (2008)
  - <http://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/>
- Strange snafu misroutes domestic US Internet traffic through China Telecom
  - <https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/>
- China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking
  - <https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca>

# BGP problemi

- BGP Stream: aktualne informacije i vizualizacije BGP problema („hijacks”, „leaks”, „outages”)
  - <https://bgpstream.com/>



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost aplikacijskog sloja



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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.

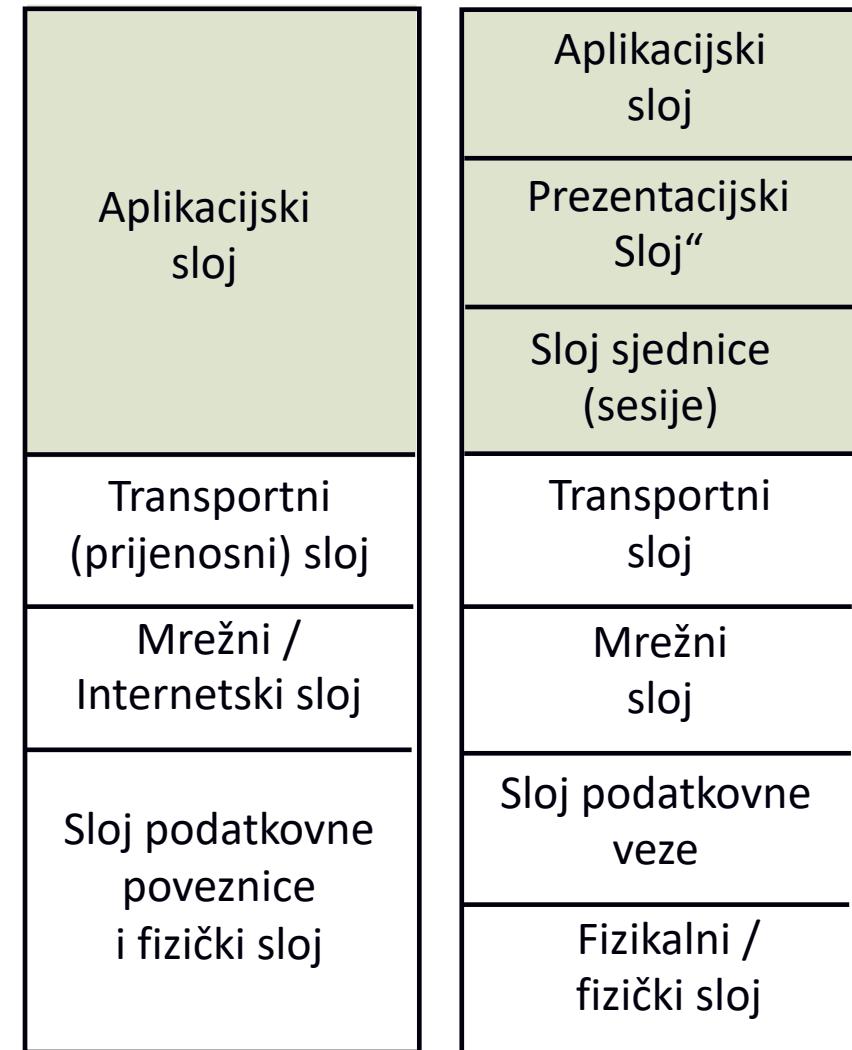
Tekst licencije preuzet je s <http://creativecommons.org/>.

# Sadržaj

- općenito o aplikacijskom sloju
- metode otkrivanja aplikacija na mrežnim čvorovima
- česti sigurnosni problemi s aplikacijama
- aplikacije za udaljeni rad

# Općenito o aplikacijskom sloju

- mnoštvo različitih aplikacijskih protokola
  - ne smije se miješati pojam aplikacije i aplikacijskog protokola
  - najčešći model usluge klijent-poslužitelj
- aplikacijski protokoli za prijenos koriste kombinaciju komunikacijskog protokola i dobro poznatih pristupa (engl. well known ports)
  - IETF aplikacijski protokoli imaju rezerviran pristup
    - korisnici aplikacija mogu koristiti i druge ako žele
  - vlasnički aplikacijski protokoli nemaju rezerviran pristup



# Vidljivost aplikacija na mrežnom čvoru (1)

- Poslužiteljske aplikacije osluškuju zahtjeve na dobro poznatim pristupima
  - Pristupi su brojevi od 1 do 65535 (za svaki prijenosni protokol: TCP, UDP, SCTP, ...)
- Administrator (ili običan korisnik) na nekom računalu korištenjem odgovarajućih alata može dobiti popis:
  - Pristupa na kojima čeka neka aplikacija
  - Poslužiteljskih aplikacija koje osluškuju zahtjeve
  - Popis statusa veza (uspostavljene ili bilo koje drugo stanje)
- Na Unix / Linux / Windows OS-u alat je **netstat**
  - Ima i mnoštvo drugih sa i bez grafičkog sučelja

# Vidljivost aplikacija na mrežnom čvoru (2)

- Primjer (izvršavanje na Linuxu)

```
$ netstat -an4
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0  0.0.0.0:22              0.0.0.0:*              LISTEN
tcp      0      0  127.0.0.1:38245        0.0.0.0:*              LISTEN
tcp      0    172  31.147.204.44:22       161.53.19.9:61407    ESTABLISHED
tcp      0      0  31.147.204.44:22       95.168.116.4:43619    ESTABLISHED
udp      0      0  0.0.0.0:5555            0.0.0.0:*
```

# Udaljeno otkrivanje aplikacija

- Temeljni način udaljenog otkrivanja aplikacija je **skeniranje pristupa** kako bi se utvrdilo koji su otvoreni
  - Najjednostavnija metoda skeniranja je pokušaj pristupa aplikaciji
  - Može se obaviti aplikacijom (Web preglednik u slučaju Weba) ili, općenitije, telnet aplikacijom u slučaju protokola TCP
- Otvoren pristup znači da je neka aplikacija prisutna
  - Samo na temelju te informacije se ne može znati koja aplikacija je prisutna.
- Potrebno je dodatno prikupljanje informacija kako bi napadač otkrio aplikaciju, i njenu verziju
  - Točna verzija je potrebna radi pronalaženja potencijalnih ranjivosti

# Otkrivanje aktivnih TCP aplikacija (1)

- Pokušaj uspostave veze (engl. TCP connect)
  - Najjednostavnija metoda koja uspostavlja u potpunosti vezu te ju odmah prekida
  - Moguće korištenje specifičnih alata ili generičke telnet naredbe
  - Upostava veze -> postoji aplikacija na pristupu, RST ne postoji
- TCP SYN skeniranje
  - tzv. poluotvoreno skeniranje (engl. half-open scanning)
  - Šalje se SYN te gleda odgovor
    - SYN+ACK znači da aplikacija sluša, čeka uspostavu veze na danom pristupu
    - RST znači da na danom pristupu ne čeka nikakva aplikacija
- U oba slučaja, ako nema odgovora tada negdje na putu postoji nekakav filter i ne znamo kakva je situacija

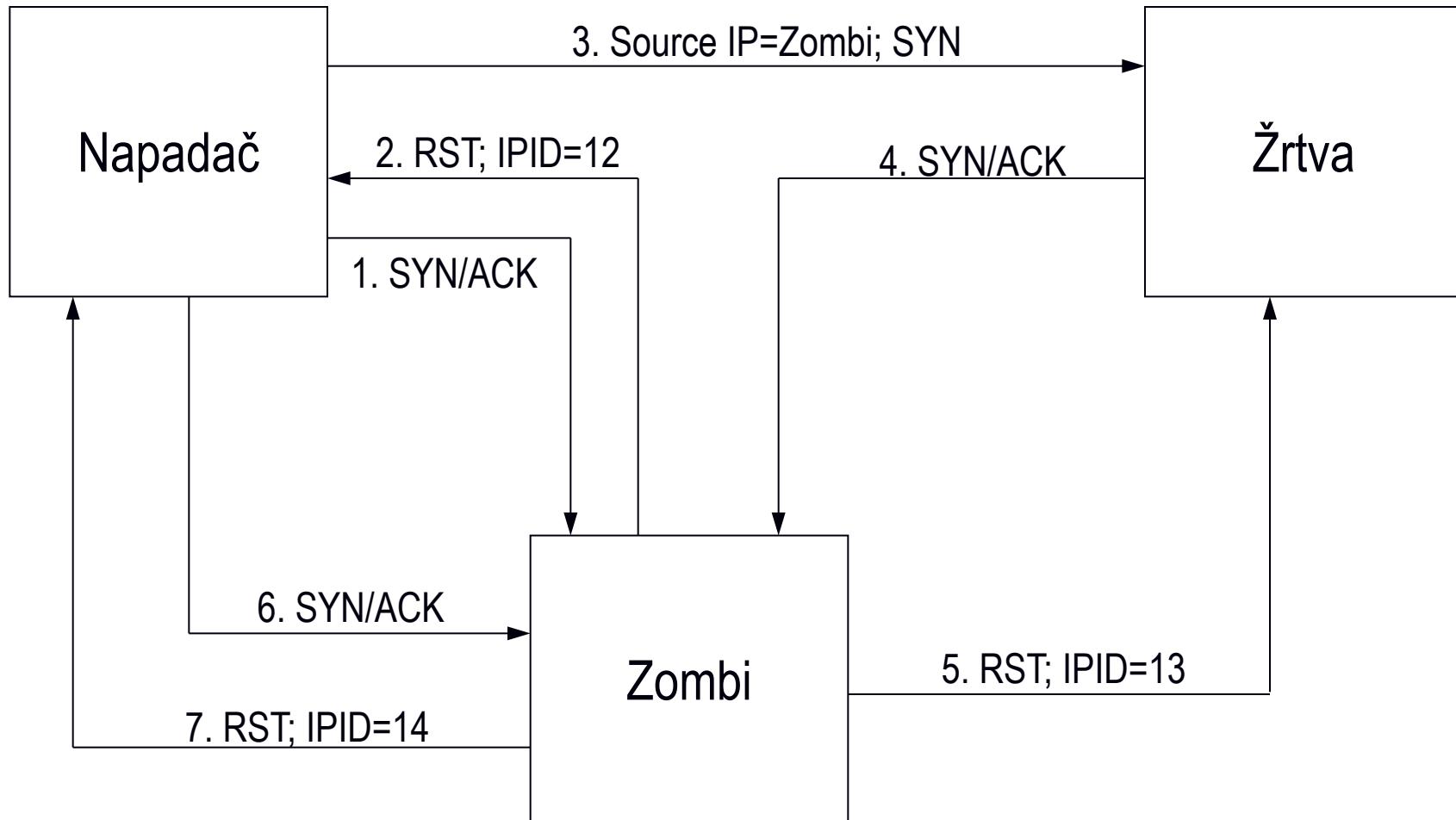
# Otkrivanje aktivnih TCP aplikacija (2)

- **TCP FIN skeniranje**
  - Šalje se segment s FIN zastavicom. U slučaju da nema ničega na pristupu, vraća se RST, u suprotnom se zahtjev ignorira
  - Određene implementacije u oba slučaja šalju RST segment
  - Sigurno možemo znati samo da nema ničega na pristupu
- **Skeniranje s fragmentacijom** (engl. fragmentation scanning)
  - Nije posebna vrsta skeniranja već mehanizam izbjegavanja detekcije
  - Fragmentiranjem IP paketa u kojemu je TCP segment otežava se detekcija skeniranja

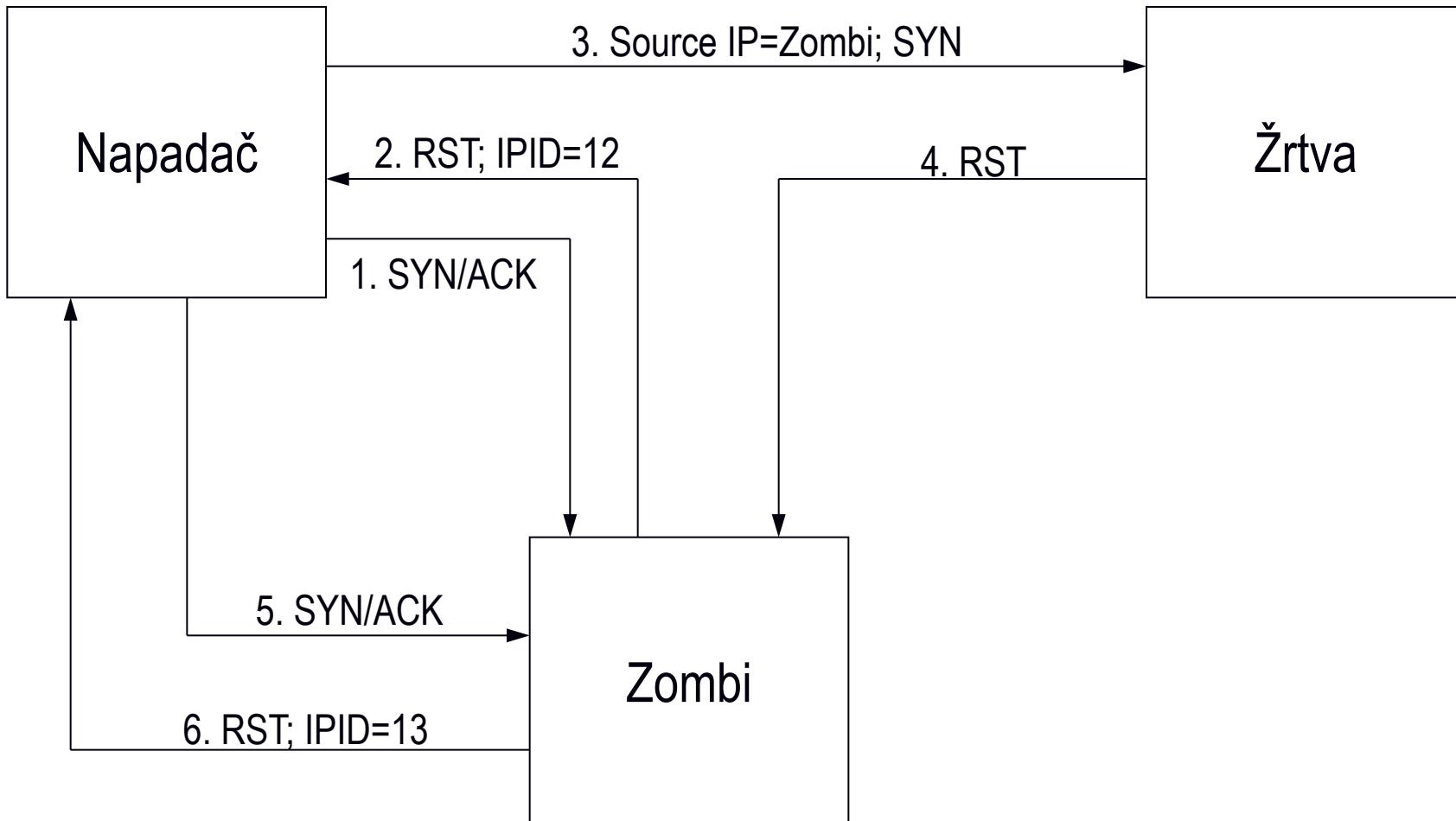
# Prikrivanje izvora skeniranja

- sva prethodna skeniranja otkrivaju lokaciju napadača
- „Idlescan” je način skeniranja korištenjem treće strane (tzv. zombi)
- očekivanja od zombija
  - mala količina prometa koju generira
  - predvidivi identifikator IP paketa (polje ID)
- ideja skeniranja
  - utvrđuje se trenutni ID koji zombi koristi
  - šalje se paket pri čemu je kao izvorišna adresa naveden zombi
  - ponovo se utvrđuje korišteni ID i na temelju toga određuje rezultat skeniranja

# „Idlescan“: ako je port otvoren



# „Idlescan“: ako je port zatvoren



# Skeniranje UDP porta (1)

- Slanje (praznog) UDP datagrama
- Za zatvoren pristup pristižu poruke “ICMP port unreachable”
  - Osim ako je negdje na putu instaliran filter
- Kada je pristup otvoren ne šalje se nikakav odgovor
  - Pod pretpostavkom da poslužitelj ignorira poruke koje nisu ispravno formatirane i nisu primljene u ispravnom redoslijedu
  - Ako se ne dobije ICMP poruka pretpostavlja se da je port otvoren
    - Što baš ne mora biti slučaj...

# Skeniranje UDP porta (2)

- Potencijalni problemi za napadača
  - UDP je nepouzdan te je potrebno pokušati nekoliko puta kako bi bili sigurni da nije došlo do gubitaka (posljedica je također da nema odgovora!)
  - Neki operacijski sustavi ograničavaju brzinu slanja ICMP poruka (RFC 1812, 4.3.2.8)
    - Generiraju ograničen broj ICMP poruka u sekundi
- Vrlo spora tehnika skeniranja

# Poteškoće sa skeniranjem za napadača

- Relativno velik broj pristupa po čvoru
  - Mora balansirati brzinu i detaljnost kako bi izbjegao otkrivanje
  - Skeniranje samo određenog podskupa pristupa
- Potencijalno velik broj čvorova koje je potrebno skenirati
  - 254 u slučaju mreže s mrežnom maskom 24
- Ako je između cilja i napadača filter ne vraćaju se odgovori i nije moguće znati je li port otvoren ili ne
- Ako je neki port otvoren ne znači da se tamo nalazi očekivana aplikacija

# Detekcija aplikacija i operacijskog sustava

- Kako bi napadač mogao iskoristiti aplikaciju koja sluša na nekom pristupu mora znati koje ranjivosti ima
  - Poznavanjem točne verzije aplikacije i koristeći baze ranjivosti može pripremiti napad na aplikaciju
  - Slično vrijedi i ako traži novu ranjivost
  - Određene aplikacije izvršavaju se na više operacijskih sustava pa je dobro znati i koji je operacijski sustav korišten
- Napad je moguć i na operacijski sustav, za što je potrebno također znati točnu verziju operacijskog sustava
  - „OS fingerprinting”

# Detekcija aplikacije

- Napadač se spaja na port
  - Neke aplikacije objavljaju svoju verziju u pozdravnim porukama koje šalju odmah po spajanju
  - Koristeći očekivani protokol pokušava komunicirati s aplikacijom
    - Na taj način utvrđuje da prepostavljena aplikacija čeka na pristupu
    - Moguće je na temelju konverzacije s aplikacijom utvrditi verziju
- Problemi za napadača
  - Ako aplikacija ne objavljuje svoju verziju/tip ili objavljuje neku generičku ili lažnu verziju
  - Na aplikacije se stavljaju zakrpe (patch) koje ne mijenjaju prijavljenu verziju aplikacije
  - Funkcionalnosti iz novijih verzija se dodaju na starije (a s njima i ranjivosti) pri čemu se također ne mijenja prijavljena verzija

# Otkrivanje vrste i verzije operacijskog sustava

- „OS fingerprinting”
  - Norme i specifikacije protokola ne definiraju absolutno svaki detalj ponašanja implementacije
    - Kada se implementira protokol odabire se različita ponašanja – slučajno ili namjerno
    - Iz verzije u verziju također se nadograđuje mrežni stog te mu se mijenja ponašanje
  - Detekcija OS-a temelji se snimanju ponašanja njegova mrežnog stoga te usporedbi s bazom poznatih operacijskih sustava
  - Detekcija nije u potpunosti pouzdana, tj. uvijek postoji mogućnost pogreške
    - snimljenom ponašanju odgovara više operacijskih sustava!

# Primjer alati za skeniranje: nmap

```
# nmap -O 31.147.204.44
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

# Česti sigurnosni problemi s aplikacijama

- pogađanje vjerodajnica i drugih informacija
  - najčešće pogađanje grubom silom
  - neispravno rukovanje lozinkama
- korištenje nezaštićene komunikacije
- ranjivosti u aplikaciji aplikacije koje omogućavaju njenu zloupotrebu

# Napadi pogađanja grubom silom

- Pokušaj otkrivanja nepoznate ili tajne informacije upotrebom pogađanja (engl. brute force)
  - Najčešće se pograđaju lozinke
  - Pogađanje korisničkih imena, dijeljenih tajni,...
- Sve usluge (engl. services) koje omogućavaju prijavu putem mreže ranjive su na pogađanje
  - telnet, ftp, r\* naredbe, ssh, http, snmp, ...
- Napad pogađanja može biti „on-line” ili „off-line”
  - „on-line” uključuje interakciju s uslugom
  - „off-line” radi na ukradenim podacima

# Zaštite od pograđanja grubom silom

- Ograničavanje pristupa usluzi
- Kvalitetne, jake lozinke (dobra entropija!)
  - Nametati ograničenja kompleksnosti lozinke
  - Koristiti fraze (passphrases) umjesto lozinki
- Ograničavanje broja pokušaja, zaključavanje
  - Ubacivanje kašnjenja između dva pokušaja
  - Nakon N pokušaja privremeno ili permanentno zaključavanje korisničkog računa
- Primjena jačih autentifikacijskih metoda (PKI, 2FA, ...)
- Pohrana lozinki u šifriranom obliku ili u obliku sažetka
  - Zaštita od „off-line“ pograđanja

# Nekorištenje šifrirane komunikacije

- Mnogi protokoli šalju podatke preko mreže u čistom obliku
  - Snimanjem prometa moguće je ukrasti osjetljive podatke
  - Dosta često slanje lozinke preko mreže
- Mnogi aplikacijski protokoli su ranjivi na prislушкиvanje
  - Posebno su kritični aplikacijski protokoli temeljeni na UDP-u
    - TLS se ne može koristiti, a DTLS nije toliko zaživio
- Zaštite
  - Šifriranje na nižim slojevima (IPsec, TLS)
  - Tuneliranje korištenjem aplikacije SSH ili neke slične metode
  - Korištenje autentifikacijskih protokola koji ne prenose lozinke preko mreže
  - Noviji protokoli razvijaju se s „ugrađenom“ enkripcijom, npr. QUIC/HTTP3

# Ranjivosti implementacija Internet usluga

- značajan broj infrastrukturnih usluga Interneta implementiran je u programskim jezicima C/C++
  - jezici niskog nivoa u kojima je vrlo lako uvesti ranjivost
- niz čestih ranjivosti – neki specifični za C/C++ a neki općeniti
  - preplavljanje spremnika (engl. buffer overflow), pisanje van granica polja
  - problemi sa nizovima za formatiranje
  - dvostruko oslobođanje radne memorije (engl. double free)
  - pogreške u aritmetičkim operacijama („krivi“ tipovi podataka)
  - ... i niz drugih

# Posljedice ranjivosti

- infrastrukturne usluge dostupne su na Internetu
  - šaljući posebno formatirane zahtjeve napadač pokušava iskoristiti ranjivosti
  - određene ranjivosti nisu dostupne putem mreže već samo lokalno – tada se koriste za podizanje privilegija jednom kada se dobije pristup računalu
- usluge/aplikacije izvršavaju se s nekim privilegijama, često i administratorskima
  - ovladavanjem usluge napadač preuzima njene ovlasti, moguća potpuna kontrola poslužitelja na kojemu se izvršava usluga
- napadači iskorištavaju ranjivosti korištenjem tzv. „shellcode-a”
  - kratak kod, s vrlo specifičnim uvjetima rada, zadaća mu je pokrenuti nešto drugo – primjerice pokrenuti proces za udaljeni pristup

# Neke općenite zaštite

- dobar dizajn programa sa uključenom sigurnošću od samog početka
- pisanje koda pazeći da se ne uvode ranjivosti
- izbjegavati izvršavanje Internet usluga s administratorskim ovlastima
  - postoje još dodatni mehanizmi ograničavanja prava procesa
- nadogradnja aplikacija čim se otkriju ranjivosti
  - CVSS je jedna korisna mjeru za određivanje opasnosti od ranjivosti
- isključivati nepotrebne usluge
- ograničavati pristup uslugama

# Primjer: Preplavljanje spremnika

- mehanizam ranjivosti
  - programer alocira određenu količinu prostora za prihvat podataka s mreže
    - na stogu (stack overflow) ili na gomili (heap, heap overflow)
  - napadač namjerno šalje veću količinu podataka te se podaci moraju prepisati van predviđenog prostora – prepisuju nešto drugo
    - „nešto drugo“ su nekakvi parametri na stogu, primjerice povratna adresa
  - po povratku iz funkcije izvršava se napadačev kod (shellcode)
  - napadačev kod izvršava neku akciju koja omogućava pristup napadaču
- zaštita
  - pažnja prilikom pisanja koda, korištene zaštitnih mehanizama, izbjegavanje nesigurnih funkcija
  - korištenje neizvršivog stoga i gomile

# Poslužitelji elektroničke pošte

- Elektronička pošta koristi barem dva poslužitelja
  - MTA - Mail Transfer Agent (postfix, sendmail, qmail, ...)
  - MUA - Mail User Agent / MDA - Mail Delivery Agent (dovecot, ...)
- Danas je uobičajeno integrirano rješenje (tzv. groupware)
  - MS Exchange, Zimbra, Lotus Notes
  - Značajno povećana kompleksnost sustava što znači i vjerojatnije pogreške
  - Mogućnost korištenja jednostavnijeg posredničkog poslužitelja radi sigurnosti
- Poslužitelj elektroničke pošte direktno izložen na Internetu
  - Sprečavanje pristupa bi onemogućilo primanje elektroničke pošte
- Obavezna redovita nadogradnja

# Usluga prijenosa datoteka (1)

- Originalno za tu namjenu bio je predviđen protokol FTP
  - File Transfer Protocol
- Jedna od primjena je anonimni „upload” i „download” datoteka
  - Neispravnim podešavanjem moguće je napadačima omogućiti postavljanje nedozvoljenih sadržaja, dohvat postojećih „skvirenih” datoteka, brisanje sadržaja, čitanje i pisanje direktorija na poslužitelju kojima se ne bi smjelo pristupiti
  - Napadači su znali razmjenjivati piratizirani materijal zloupotrebom anonimnih FTP poslužitelja
- Nema zaštitu komunikacije, prijenos lozinke preko mreže
  - Postoji ekstenzija FTPS, ali se ne koristi često

# Usluga prijenosa datoteka (2)

- Protokol **uključuje otvaranje zasebnih TCP veza!**
  - Kontrolni kanal koristi jednu TCP vezu, za svaki prijenos podataka otvara se zasebna TCP veza
  - Otvaranje zasebne veze može biti u aktivnom i pasivnom modu
    - Aktivni način -> poslužitelj se spaja na klijenta
    - Pasivni način -> klijent se spaja na poslužitelj
- Povećava **kompleksnost** uređaja vatrozid/NAT
- Preporuka: izbjegavati
  - Alternativa SFTP/SCP
  - Ne koristiti anonimni pristup

# Usluga nadzora mreže

- SNMP – Simple Network Management Protocol
  - udaljeni nadzor (i upravljanje) usmjernika, preklopnika, poslužitelja,...
  - nema kriptografsku zaštitu, koristi UDP
  - mogućnost DoS ili udaljenog izvođenja naredbi
- zaštita
  - provjeriti sve uređaje u mreži koji imaju omogućen SNMP (npr. SNScan)
  - onemogućiti SNMP na svima uređajima na kojima nije nužan
  - instalirati najnovije zakrpe, „firmware update”
  - promijeniti podrazumijevane „public” i „private community”
  - izolirati u zaseban VLAN te vatzrozidom ograničiti pristup
  - koristiti SNMPv3

# Udaljeni rad

- Najpoznatiji protokol: SSH
  - Zamijenio telnet, r naredbe (rsh, rlogin, rcp), ftp
  - OpenSSH – najpoznatija implementacija, otvorenog koda, Unix/Linux, Windows
  - PuTTY – poznati klijent na Windows operacijskom sustavu
  - WinSCP – za prijenos datoteka na Windows OS-ovima
- Postoje i komercijalne implementacije (SecureCRT)
  - U odnosu na OpenSSH jedina prednost je GUI sučelje

# Slojevi protokola SSH

<b>SSH User Authentication Protocol</b> autentifikacija klijenta poslužitelju	<b>SSH Connection Protocol</b> multipleksiranje šifriranih tunela u nekoliko logičkih kanala
<b>SSH Transport Layer Protocol</b> autentifikacija poslužitelja, povjerljivost i integritet podataka te optionalno komprimiranje podataka	
<b>TCP</b> pouzdana konecijski orijentirana dostava s kraja na kraj	
<b>IP</b> (nepouzdana) dostava datagrama kroz mrežu	

# SSH Transport Layer Protocol

- Dogovara način razmjene ključeva, asimetrični algoritam šifriranja, simetrični algoritam šifriranja, algoritam za autentifikaciju poruka i algoritam kriptografskog sažetka
  - klijent i poslužitelj razmijene uređene liste podržanih algoritama
  - odabire se prvi algoritam koji se nalazi na popisu klijenta, a ujedno je podržan od strane poslužitelja
  - ako se ne može pronaći zajednički algoritam, veza se prekida

# SSH Transport Layer Protocol

- Autentifikacija poslužitelja korištenjem para ključeva (javni/privatni)
  - poslužitelj može imati više ključeva za različite asimetrične algoritme
  - više poslužitelja može dijeliti isti ključ
- Prilikom prvog spajanja klijentski program korisniku prikazuje sažetak poslužiteljskog ključa
  - Od korisnika se očekuje provjera ispravnosti sažetka kako bi se spriječio MITM
  - Nakon provjere korisnik bi trebao potvrditi ispravnost sažetka ključa (Leap of faith)
  - Klijentski program zapisuje ključ lokalno i više ga ne predočava korisniku, ali ga obavezno provjerava prilikom svakog spajanja  
~/.ssh/known\_hosts

# Podržane autentifikacije klijenta

- Prijava upotrebom korisničkog imena i lozinke
- Upotreba asimetrične kriptografije
  - Klijent generira par javni-tajni ključ
  - Tajni ključ može i treba biti zaštićen lozinkom
  - Javni ključ instalira na svako računalo kojemu želi pristupiti (~/.ssh/authorized\_keys)
- Podržano je još
  - PKI, Kerberos, PKCS11, integracija s PAM sustavom na Linuxu, 2FA, ...

# Usluge temeljene na protokolu SSH

- Udaljen rad (ssh klijent)
- Prijenos datoteka (scp i sftp klijenti)
- Tuneliranje Ethernet okvira ili IP datagrama
  - Ostvarivanje VPN-ova na drugom ili trećem sloju
- Prosljeđivanje (engl. forwarding) lokalnih i udaljenih pristupa
  - Spajanjem na lokalni pristup otvara se veza na udaljenom računalu prema nekom drugom pristupu/IP adresi (prosljeđivanje lokalnog pristupa)
  - Spajanjem na pristup udaljenog računala otvara se veza na neki pristup lokalnog računala (prosljeđivanje udaljenog pristupa)

# Načini korištenja

- udaljeni pristup:

```
ssh user@host
```

- interaktivna naredba:

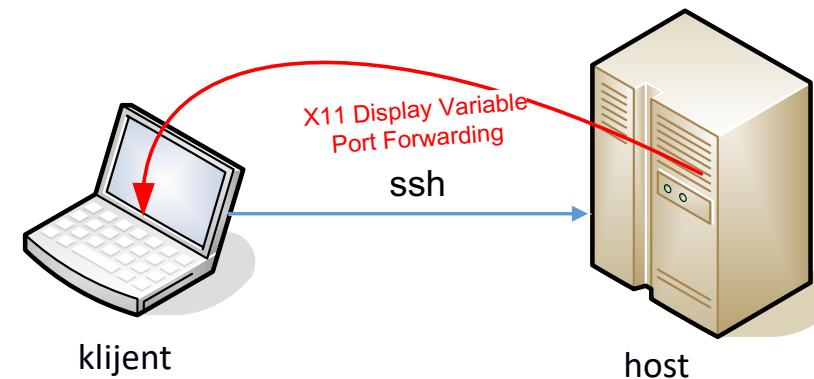
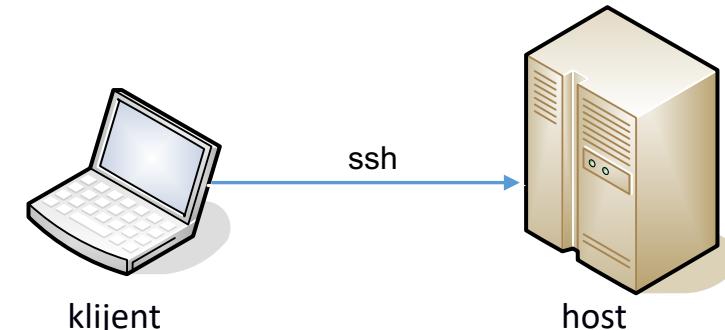
```
ssh -t user@host naredba
```

- X11 naredba:

```
ssh -X user@host Xnaredba
```

- za verzije novije od OpenSSH 3.8p1:

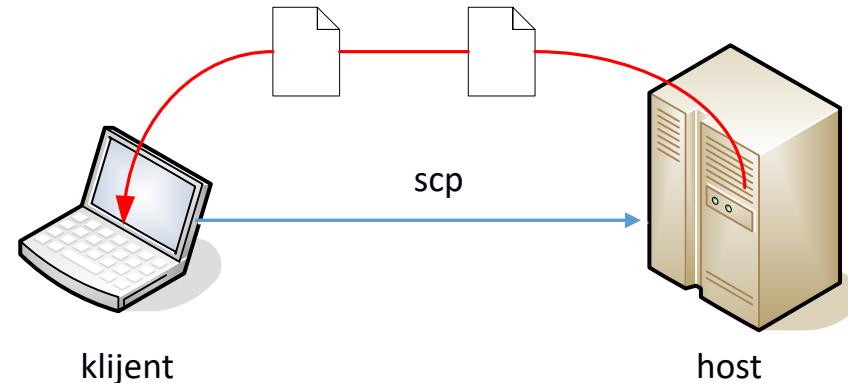
```
ssh -Y user@host Xnaredba
```



# Kopiranje datoteka

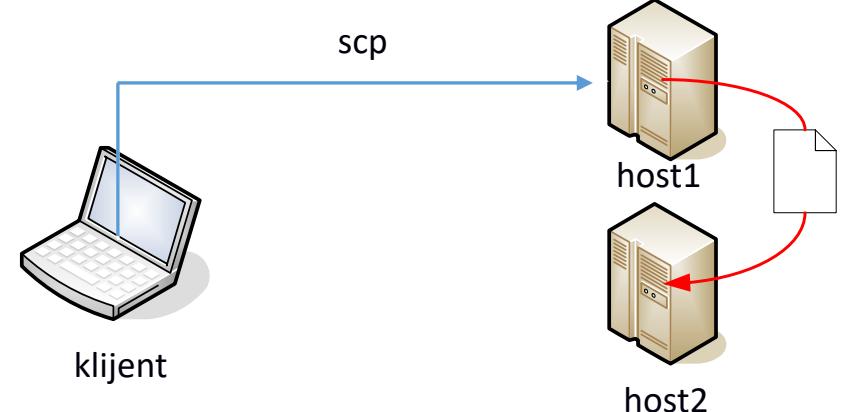
- kopiranje na lokalno računalo:

```
scp user@host:src_path dest_path
```



- kopiranje na udaljeno računalo:

```
scp src_path user@host:dest_path
```



- kopiranje s host1 na host2:

```
scp user@host1:src_path user@host2:dest_path
```

# Host ključevi

- ključevi se koriste za verifikaciju autentičnosti udaljenog računala
- javni ključevi provjerenih računala:  
/etc/ssh/known\_hosts  
~/.ssh/known\_hosts
- poruka prilikom prvog spajanja

```
$ ssh mrepro.tel.fer.hr
```

The authenticity of host 'mrepro.tel.fer.hr (161.53.19.47)' can't be established.

RSA key fingerprint is SHA256:vV4ju0F3SbDzJa3g7SWEx8DRhg+7XP0r/c7+nMQzWBg.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'mrepro.tel.fer.hr,161.53.19.47' (RSA) to the list of known hosts.

- sadržaj datoteke ~/.ssh/known\_hosts:

```
mrepro.tel.fer.hr,161.53.19.47 ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAQABAAQC+YGIJbtrzLhSy1qu+c6/38DRFGG0f/PPeiNtfReYIQ1CquiUU4rSCWeL7xQjtA5Kh
O/0Ej6vzkMr4k0ANsviDJ1NgweOUJNo/DVZv+YreNjm1EZH350O43CH17Eo5VphNi+5KdGeartpTESNt/Dv+ACtMGpra5Gg+
ELLaBkovG/YgzswTGdk+UZ4xA1ONg/4dEGF7dvYoXqqG9kpvmeeZ+R37vKBRQJ8RT4U0J+YCJBsGcGi2FilUMFdfe/JUmH6Y5
aH5HwhM20e/2DQY6p7kMMjm2p6UaAbAUkrgyGEBPyO6tsuf6vopl7GVxGqeMN9EB0H4ve5J9AFoc5FouZKI
```

# Korisnički ključevi

- autentifikacija korisnika računalu

RSA:

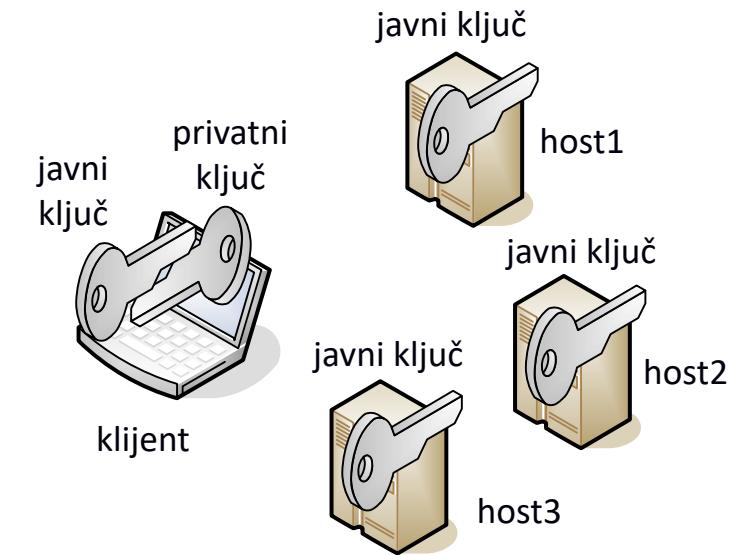
ključevi: `~/.ssh/id_rsa`, `~/.ssh/id_rsa.pub`  
`$ ssh-keygen -t rsa`

DSA:

ključevi: `~/.ssh/id_dsa`, `~/.ssh/id_dsa.pub`  
`$ ssh-keygen`

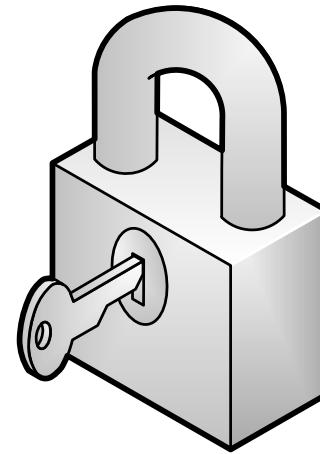
ECDSA:

ključevi: `~/.ssh/id_ecdsa`, `~/.ssh/id_ecdsa.pub`  
`$ ssh-keygen -t ecdsa`

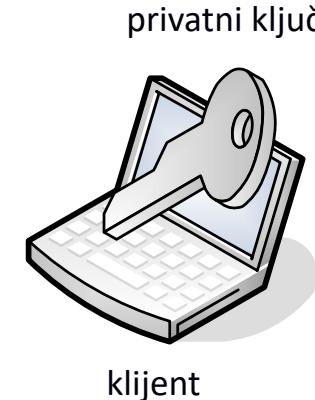


# SSH agent

- SSH agent pohranjuje otključanu kopiju ključeva  
  \$ eval `ssh-agent`
- u pravilu se počeće automatski (startup)
- može se prosljeđivati na drugo računalo
- dodavanje ključeva:  
  \$ ssh-add



ssh-agent



klijent

# Port forwarding

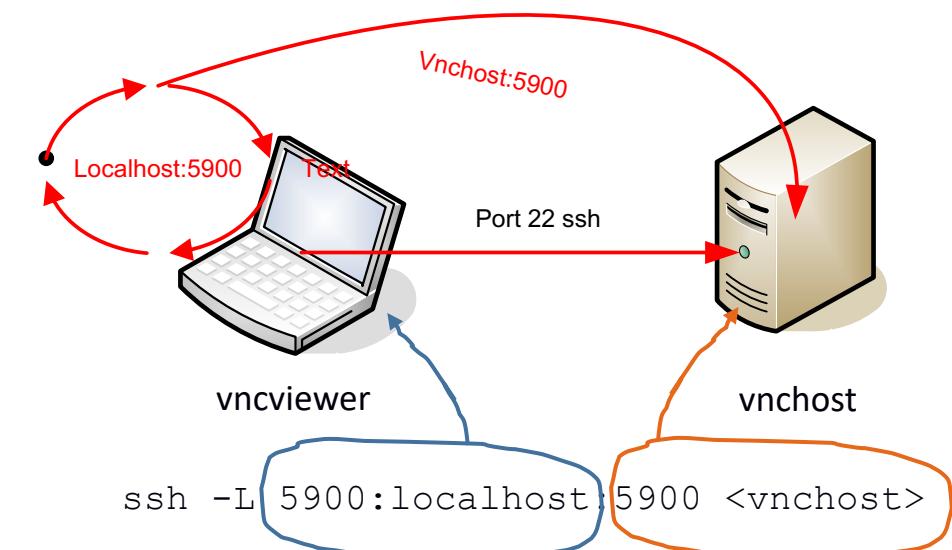
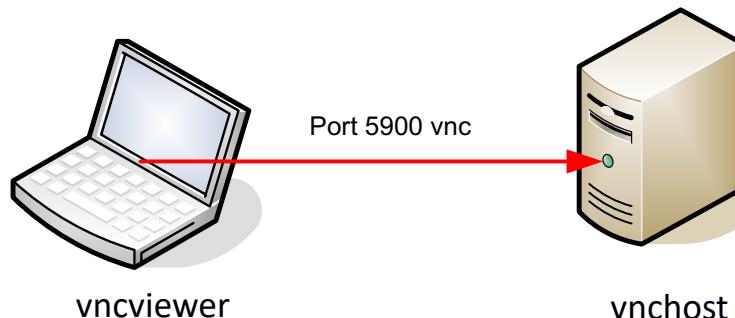
- local forwarding:

```
ssh -L <localport>:<targethost>:<targetport> <ssh_host>
```

- primjer - osiguravanje VNC komunikacije:

```
$ ssh -L 5900:localhost:5900 <vnchost>
```

```
$ vncviewer localhost
```



# Mogući operativni problemi sa SSH

- Korisnik nije zaštitio tajni ključ lozinkom
  - Omogućava napadaču neometan pristup svim računalima na koje se može prijaviti bez lozinke
  - To je posebno kritično kada se pristupa administratorskim računima, i/ili se tajni ključ nalazi na slabije zaštićenim radnim stanicama administratora
- Popis računala i javnih ključeva
  - Omogućava napadaču enumeraciju računala bez velikog problema
  - U novijim verzijama pohranjuje se sažetak imena računala
- Zamjena i povlačenje ključeva je zahtjevna
  - Primjerice kada netko ode iz tvrtke



SVEUČILIŠTE U ZAGREBU



Diplomski studij

Ak. godina 2022./2023.

# Sigurnost komunikacija

Vatrozid  
IDS



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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

- Firewall
- IDS

# Pregled

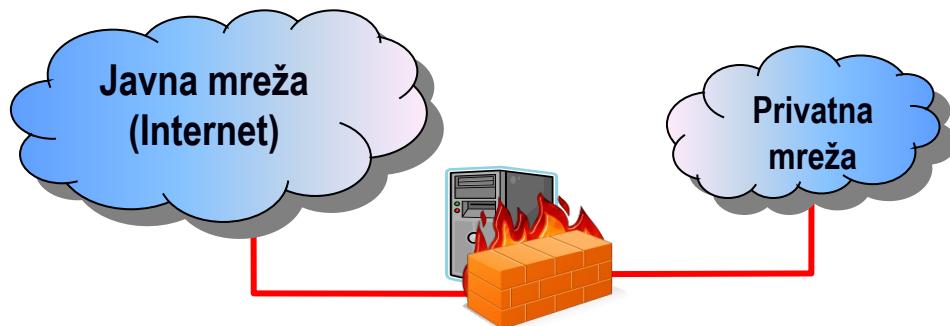
- „Defense in Depth” – sveobuhvatna zaštita
  - perimetar, unutarnja mreža, ljudski faktor
- „Perimeter Security”
  - perimetar - “prednji kraj kružne obrane”
- perimetar uključuje:
  - usmjeritelje
  - **vatrozid** (engl. firewall, sigurnosna stijena)
  - IDS (Intrusion Detection System – sustav za otkrivanje uljeza)
  - VPN (Virtual Private Network)
  - softverska arhitektura
  - DMZ & „Screened Subnet” (oklopljena podmreža)

# Zaštita lokalne mreže vatrozidom

- pretpostavka
  - lokalnoj mreži se vjeruje!
  - vanjska mreža je potencijalno opasna
- nezaštićena mreža
  - sigurnost mora biti implementirana na svakom pojedinom računalu
  - jedno ranjivo računalo narušava sigurnost cijele mreže
  - noćna mora administratora!
- zaštićena mreža
  - na granici između vanjske (opasne) i unutarnje (sigurne) mreže postavlja se vatrozid
  - vatrozid omogućava kontrolu pristupa
  - pomaže nadzoru sustava i pojednostavljuje upravljanje

# *Firewall – vatrozid, sigurnosna stijena*

- mrežni uređaj koji dopušta, zabranjuje ili prosljeđuje mrežne konekcije u skladu sa sigurnosnom politikom
  - hardverski ili softverski
- kontrola prometa između mreža s različitim stupnjevima povjerenja (Internet ↔ privatna lokalna mreža)



# Osnovni princip rada vatrozida

- filtriranje paketa (engl. packet filtering) - filtrira promet na različitim slojevima
  - odbacuje ili propušta pakete na temelju:
    - vrste protokola,
    - IP adrese izvorišta / odredišta,
    - brojeva portova,
    - sadržaja datagrama, ...
- posredničke (engl. proxy) usluge
  - programi koji komuniciraju s vanjskim poslužiteljima umjesto internih klijenata
  - 2 komponente: *proxy* poslužitelj i klijent
  - prosljeđuje samo dozvoljene upite

# Ograničenja

- nije krajnje rješenje problema sigurnosti
  - ne može u potpunosti nadzirati sadržaj koji se prenosi (virusi – provjeravanje sadržaja paketa, svakodnevno nove vrste virusa)
  - nove vrste napada – novi filteri
  - ne štite od napada unutar mreže (zlonamjerni članovi unutar lokalne mreže)
  - potencijalni problemi s performansama
  - ako je vatrozid kompromitiran mreža postaje nezaštićena
  - „backdoor“ u mrežu radi nametnutih restrikcija
- sigurnosne strategije
  - dodijeliti samo nužne (najmanje potrebne) privilegije
  - obrana u dubinu
    - na svim nivoima valja instalirati dodatne sigurnosne zaštite
  - „fail-safe“
  - prestanak rada vatrozida ne smije utjecati na sigurnost sustava

# “Thinking About Firewalls”

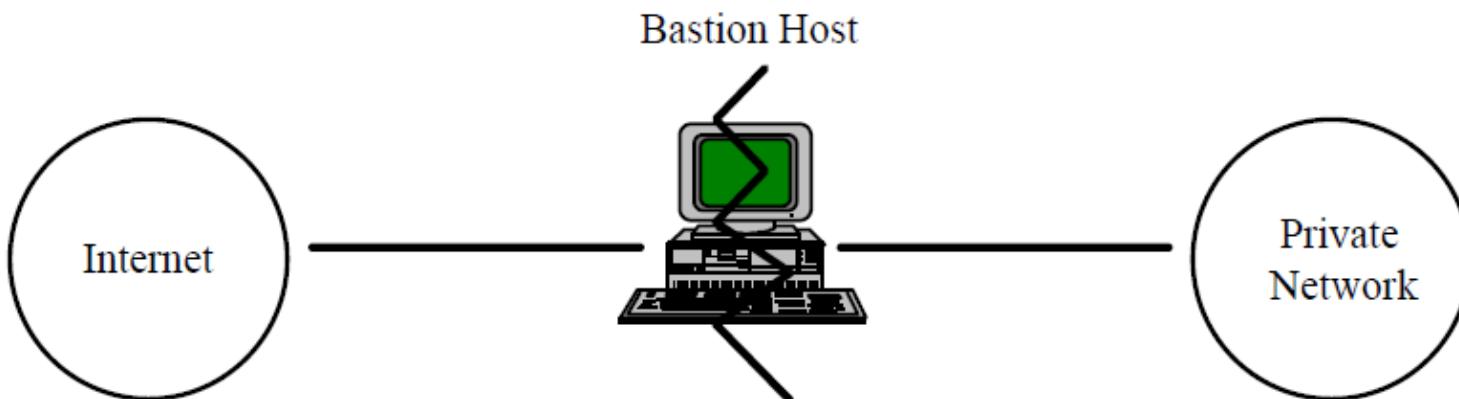
- Marcus J. Ranum, Thinking About Firewalls
  - Trusted Information Systems, Inc., Glenwood, Maryland
  - Proceedings of Second International Conference on Systems and Network Security and Management, SANS II, Washington, DC, 1993

# Terminologija

- Screening Router – zaštitni usmjeritelj
  - osnovna komponenta većine vatrozida (ponekad i jedina)
  - usmjeritelj ili računalo koje obavlja usmjeravanje uz mogućnost neke vrste filtriranja paketa
  - posjeduje mogućnost blokiranja prometa između mreža ili određenih računala na nivou IP adresa i portova
- Bastion host
  - bastion, tvrđava, utvrda
  - kritična ali dobro osigurana točka u mreži – redovito kontrolirana, nadzirana, osvježavana, često s modificiranim softverom

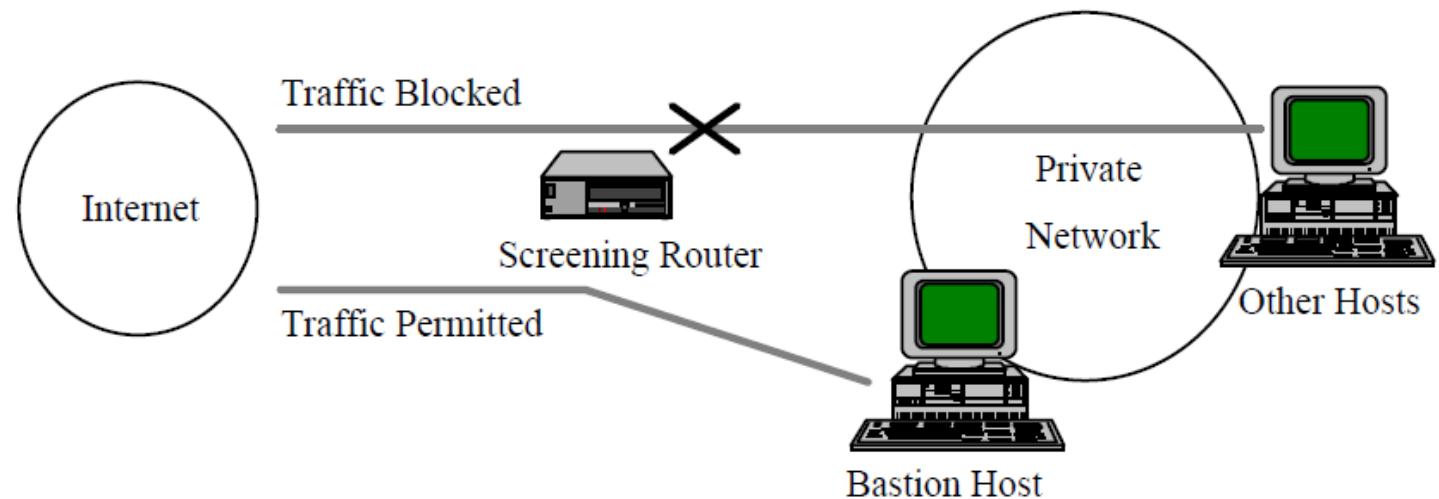
# Terminologija

- Dual Homed Gateway
  - umjesto „screening routera“ između privatne mreže i Interneta smješta se bastion host
  - onemogućeno prosljeđivanje IP datagrama
    - direktni promet između mreža je onemogućen
    - visoka razina kontrole
    - korištenje usluga preko korisničkih računa na bastion hostu ili posredničkih poslužitelja (proxy)



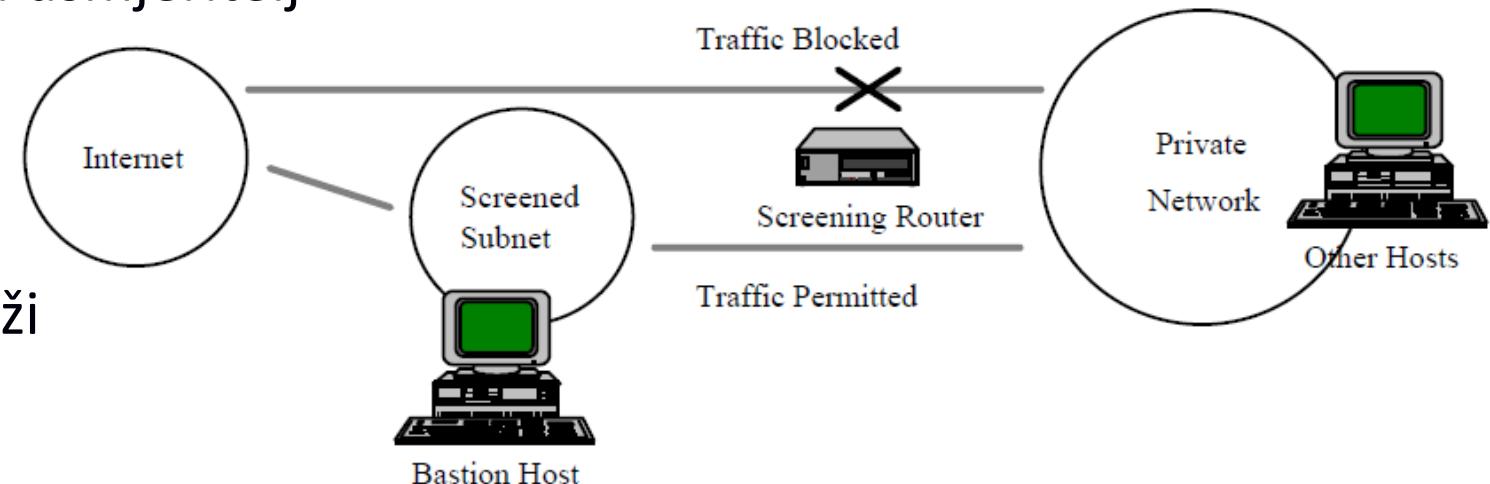
# Terminologija

- Screened Host Gateway
  - “screening router” i “bastion host”
  - “bastion host” je u privatnoj mreži i to je jedini sustav dostupan iz javne mreže – visok stupanj sigurnosti
  - omogućen pristup samo malom broju usluga
  - sav ostali promet do lokalne mreže blokiran
  - izlazne konekcije preko proxy poslužitelja



# Terminologija

- Screened Subnet
  - izolirana podmreža između Interneta i privatne mreže
  - dozvoljen pristup računalima u podmreži iz javne i iz privatne mreže
  - promet između javne i privatne mreže onemogućen
  - u pravilu unutarnji i vanjski usmjeritelj
  - ne postoji jedinstvena točka koja bi mogla kompromitirati mrežu
  - poželjno ograničiti broj usluga prema lokalnoj mreži
  - u podmreži se u pravilu nalaze bastion hostovi



# Terminologija

- DMZ - demilitarizirana zona – engl. „Demilitarized Zone”
  - područje mreže između dva filtera paketa:
    - vanjski filter propušta samo promet izvana
    - interni filter dopušta samo promet iznutra
  - odvaja vanjsku i unutarnju mrežu
  - sadrži računala koja osiguravaju:
    - vanjske usluge (npr. Web poslužitelj, DNS poslužitelj, FTP poslužitelj)
    - *Application gateway* za interne klijente
  - ako je računalo u DMZ kompromitirano:
    - unutarnji promet se ne može snimati - zaštita s internim filterom

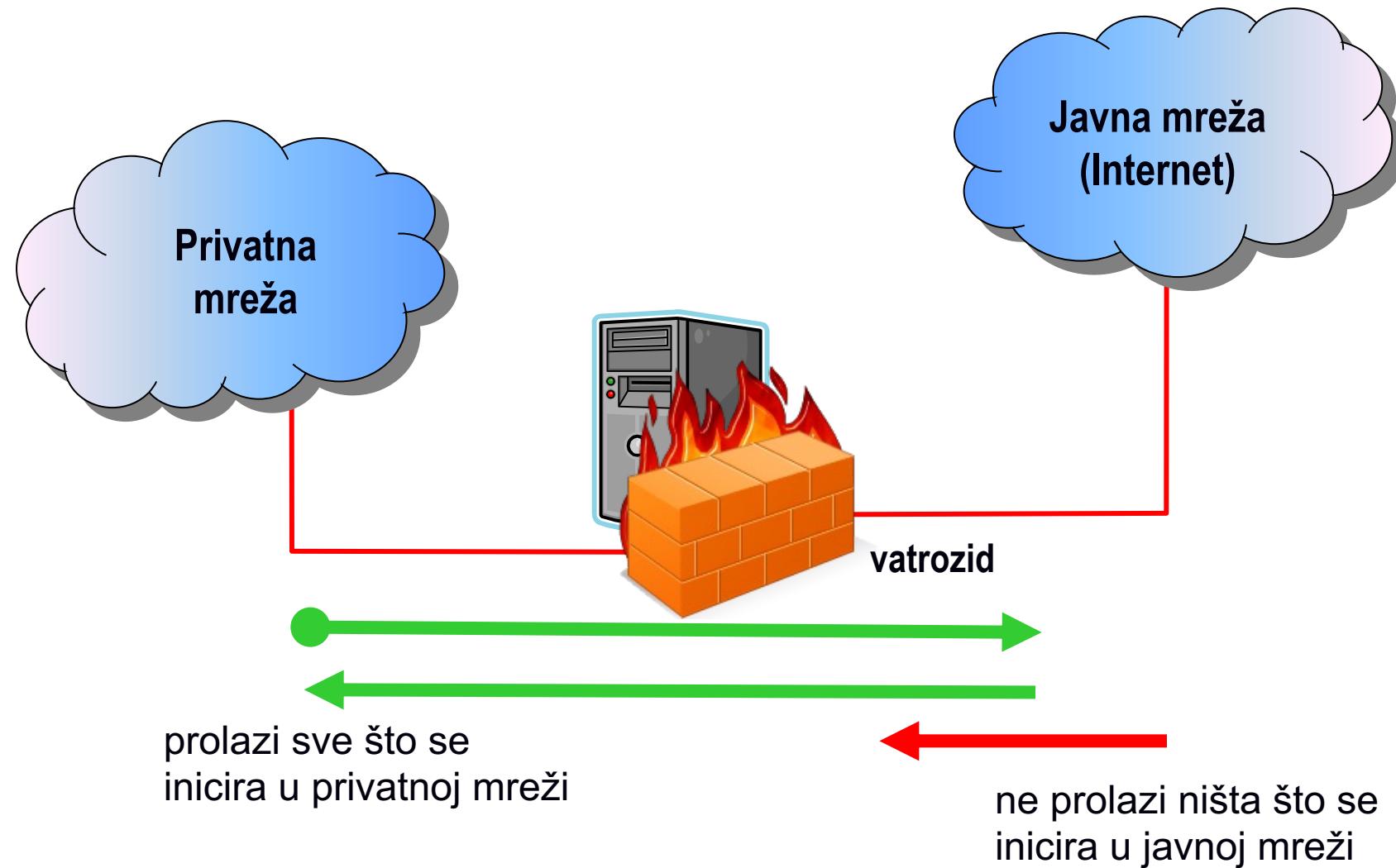
# Terminologija

- Application Gateway / Proxy Gateway - posrednik
- interpretira protokol određene aplikacije
  - na primjer HTTP / FTP
  - treba detaljno poznavati aplikacijski protokol
  - za svaki protokol potreban je novi posrednički poslužitelj (proxy)
  - može obavljati napredno filtriranje (na primjer određenih komandi)
- prednosti
  - jeftino
  - velike mogućnosti logiranja
  - unutarnja mreža je nevidljiva
- ograničenja
  - skalabilnost, performanse

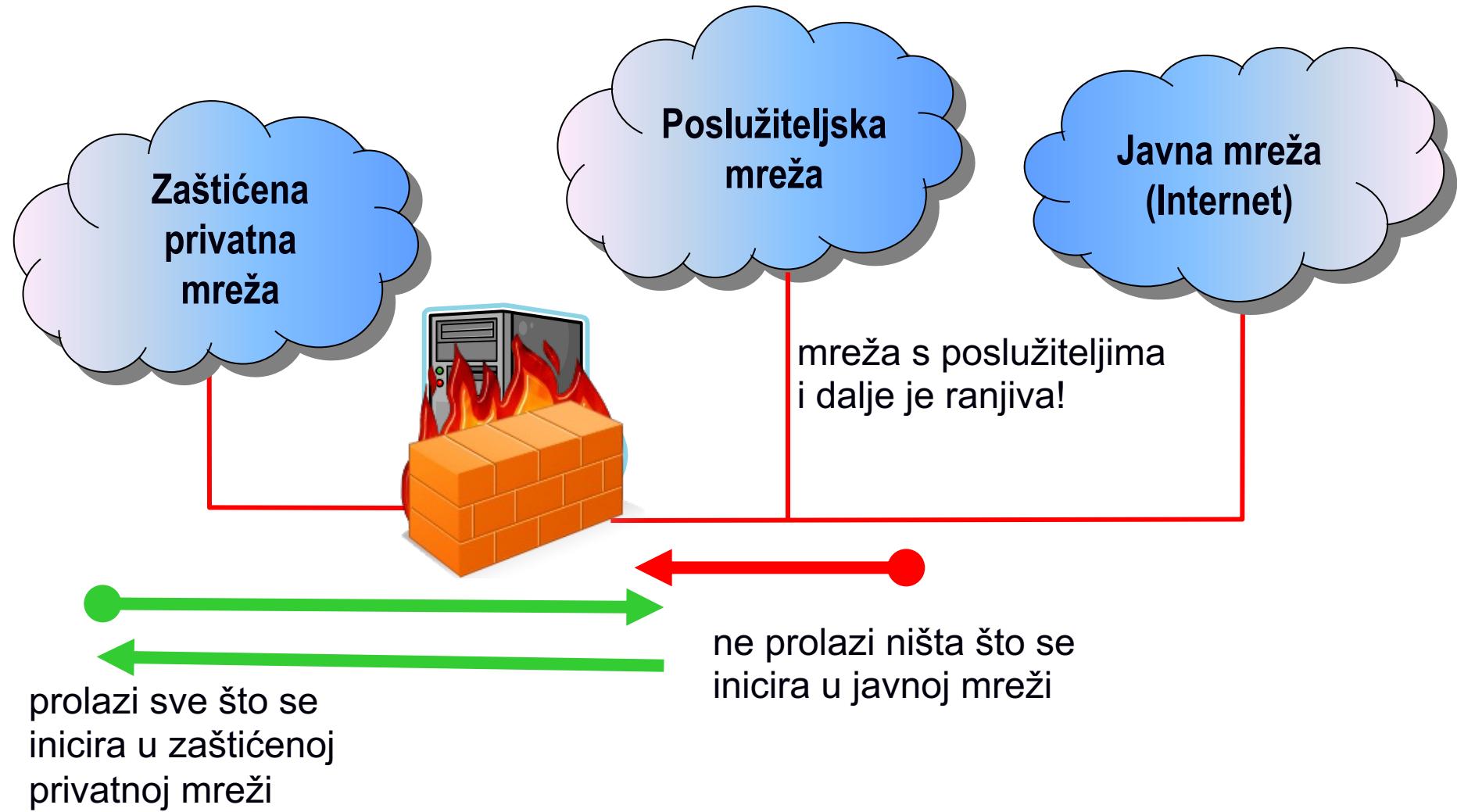
# Ostala značajna svojstva vatrozida

- kontrola štete
  - što se događa sa sigurnošću mreže ako je vatrozid kompromitiran ili uništen
- zone rizika
  - kolika je zona rizika u normalnom radu vatrozida - mjera je broj računala ili usmjeritelja koji se vide iz vanjske mreže
- ispad vatrozida
  - može li se lako detektirati: provala, uništenje
  - koliko informacija je sačuvano za naknadnu analizu napada
- jednostavnost korištenja (mreže)
- izvedba
  - zabranjeno je sve što nije izrijekom dozvoljeno
  - dozvoljeno je sve što nije izrijekom zabranjeno

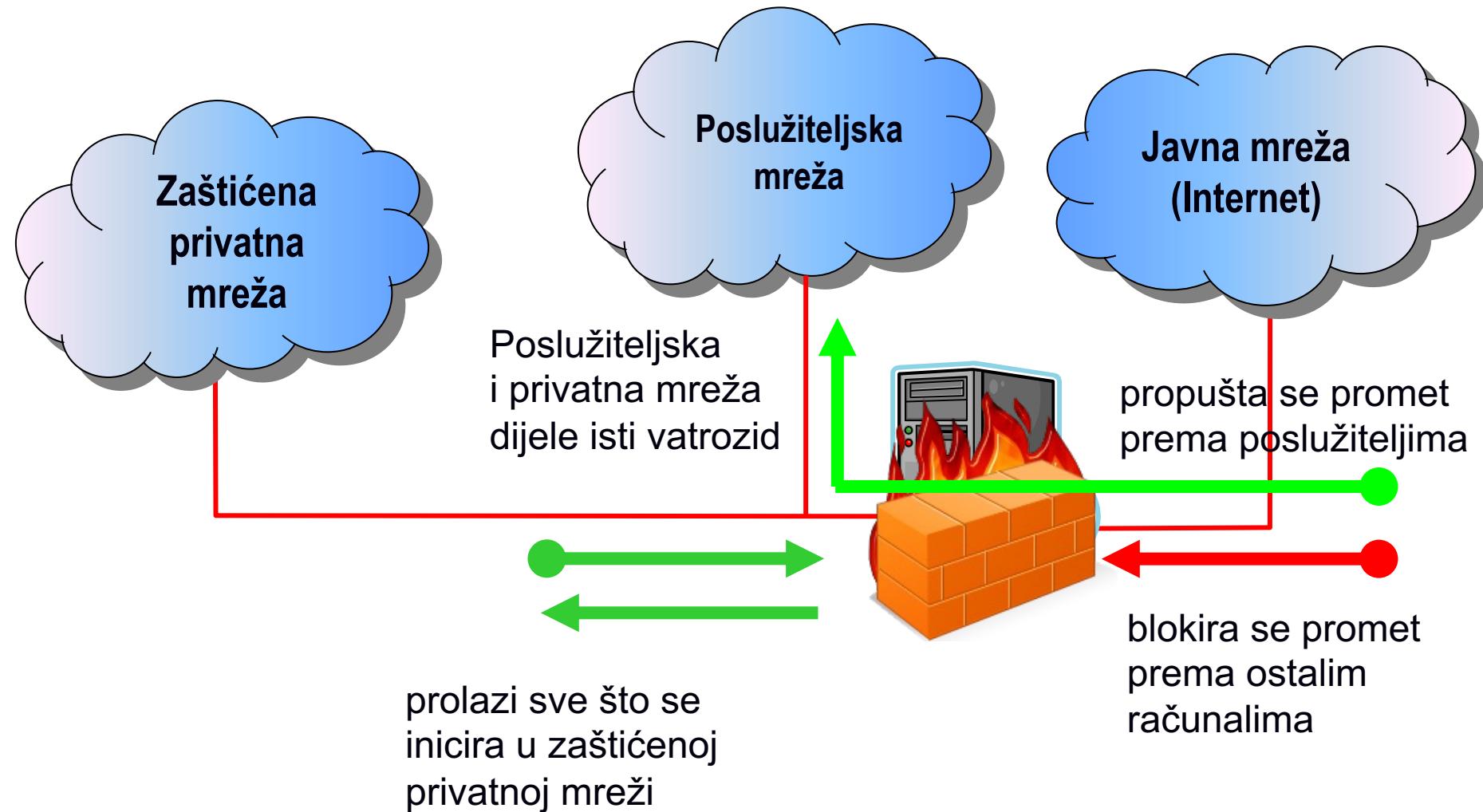
# Privatne mreže bez usluga vanjskim korisnicima



# Privatne mreže s uslugama za vanjske korisnike

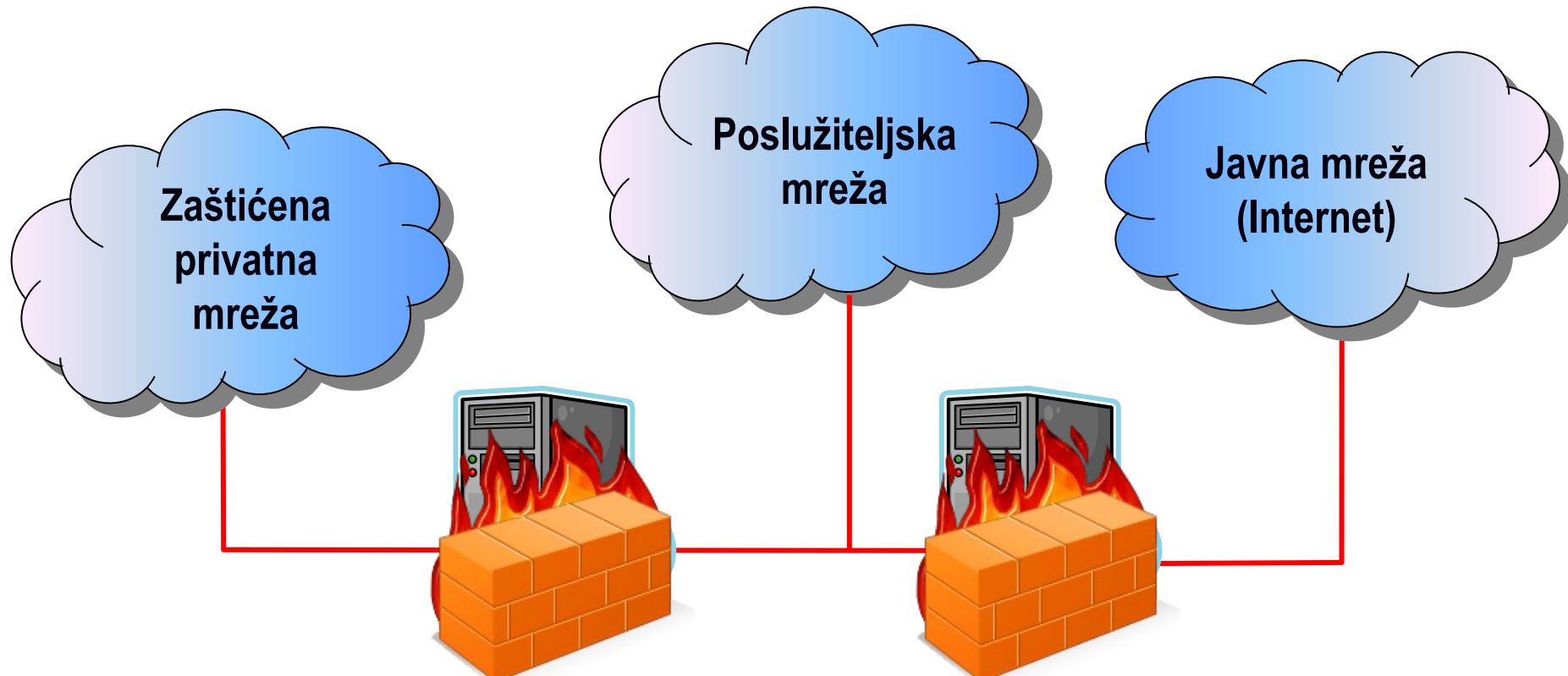


# Privatne mreže s uslugama za vanjske korisnike II



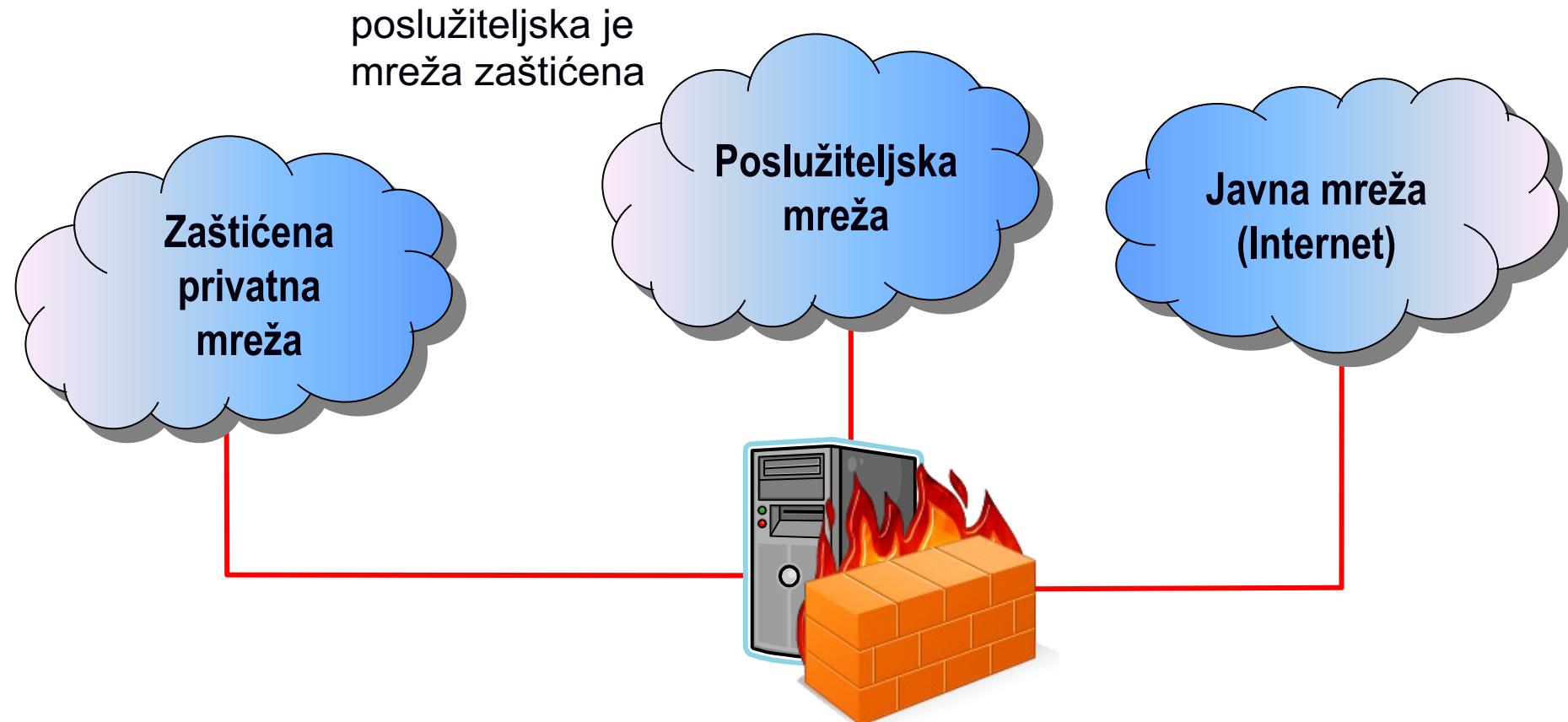
# Privatne mreže s uslugama za vanjske korisnike III

## - “Demilitarizirana zona”



poslužiteljska je  
mreža zaštićena  
dodatnim vatrozidom

# Demilitarizirana zona



# Filtriranje paketa – “*packet filter*”

- “*packet filter*” usmjerava i filtrira pakete između unutarnjih i vanjskih računala
- selektivno propušta ili blokira određene tipove paketa na temelju:
  - protokola (TCP, UDP, ICMP, ...)
  - IP adresa izvora / odredišta
  - TCP ili UDP izvorišni / odredišni port
  - TCP zastavica (SYN, ACK, FIN, ...)
  - tipa ICMP poruke
  - ...

# Pravila za filtriranje

- svako pravilo specificira:
- uzorak:
  - izvorišna adresa i broj porta
  - odredišna adresa i broj porta
  - prisustvo ili odsustvo zastavica
  - akciju (dozvoli / zabrani)
- na svaki primljeni paket pravila se primjenjuju po redu
  - ako pravilo zadovoljava postavljene uvjete izvodi se odgovarajuća akcija
  - ako niti jedno pravilo ne zadovoljava, izvodi se prepostavljena (default) akcija:
    - prihvati, propusti – Accept
    - odbaci, odbij – Reject
    - ispusti – Drop

# Filtriranje paketa

- prednosti
  - jednostavna implementacija (temelji se na postojećem hardveru)
  - dobre performanse
- ograničenja
  - ograničena provjera
  - složena konfiguracija
  - nije dovoljno fleksibilno i proširivo
  - može se zaobići tuneliranjem informacija
  - može biti ranjivo na spoofing
  - fragmentirani datagrami:
    - odbacuju se kad nema dovoljno informacija za primjenu filtra
    - ako prvi frag. sadrži dovoljno informacija ostali se propuštaju bez provjere: prvi frag. s bezazlenim vrijednostima, ostali s pomakom različitim od 0 prebrišu te vrijednosti s opasnim podacima i ponovno sastavljeni fragment se dostavlja zaštićenoj usluzi!

# *Stateful Inspection*

- radi kao paket filter (pristupne liste)
  - + održavanje stanja
    - provjera i održavanje informacije o stanju svake konekcije
- dohvaća i informacije iz protokola na višim slojevima
  - moguće je pratiti slijed sesije (na primjer za FTP)
  - virtualne sesije za beskonekijske protokole (UDP)
    - vatrozid spremi podatke o portovima korištenim u određenim UDP transakcijama
    - kreiraju se privremena pravila koja propuštaju odgovor
  - provjera svakog paketa
    - ponekad se preskače provjera paketa koji je dio uspostavljene konekcije

# Primjer vatrozida: netfilter / iptables (Linux)

- iptables se koristi za postavljanje, održavanje i provjeru pravila IP vatrozida ugrađenog u Linux kernel (netfilter)  
<https://netfilter.org/documentation/index.html#documentation-howto>
- pravila su organizirana u lance (“chains”)
  - lanci (uređene liste) se mogu pridružiti različitim fazama obrade datagrama  
[stuffphilwrites.com/wp-content/uploads/2018/09/FW-IDS-iptables-Flowchart-2018-09-01.png](https://stuffphilwrites.com/wp-content/uploads/2018/09/FW-IDS-iptables-Flowchart-2018-09-01.png)

# Primjer vatrozida: netfilter / iptables (Linux)

- „Chains“:
  - prerouting
  - input - ulazni
  - output - izlazni
  - forward - prosljeđivački
  - postrouting
  - korisnički specificirani lanci
    - dozvoljeno je „skočiti“ („jump“) na drugi lanac pravila
  - može se koristiti za implementaciju translacije mrežnih adresa (NAT)
    - source translation – masquerading
    - destination translation – port forwarding

# Filteri: *input / output / forward*

- lanac se sastoji od niza pravila koja se obrađuju slijedno
- ako paket zadovoljava zadani uzorak izvodi se definirana akcija, skok („jump“) na sljedeći lanac
- obrada završava ako se „skače“ na lance:
  - ACCEPT – paket se prihvata
  - DROP – paket se odbacuje  
(REJECT – kao DROP ali šalje icmp poruku ili tcp reset)

# Naredbe

-A, --append                        dodaj pravilo na kraj

iptables -A INPUT --dport 22 -j ACCEPT

-D, --delete                        obriši pravilo

iptables -D INPUT --dport 80 -j DROP

-I, --insert                        ubaci pravilo pod definiranim rednim brojem

iptables -I INPUT 1 --dport 80 -j ACCEPT

-L, --list                         ispisi pravila

iptables -L INPUT -n -v

-F, --flush                        obriši sva pravila definiranog lanca

iptables -F INPUT

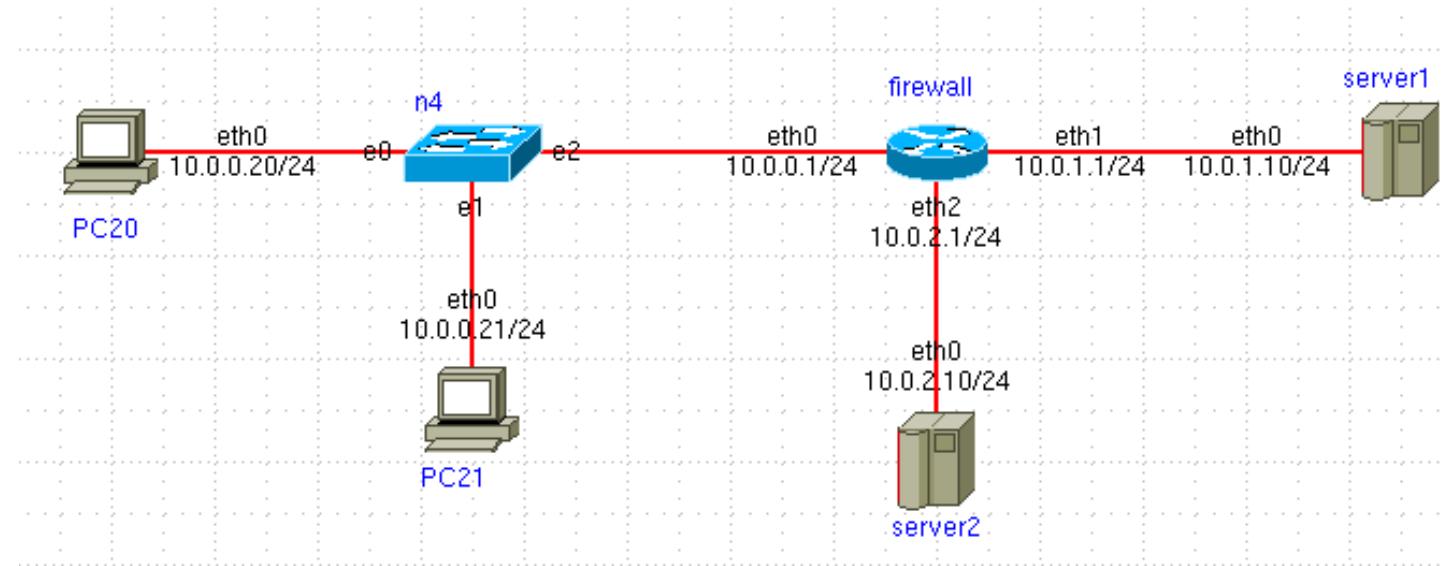
-P, -- policy                      *defaultna politika (implicitno zadnje pravilo)*

iptables -P INPUT DROP

# Uzorci u pravilima

- generički uzorci
  - p --protocol na primjer tcp, udp, icmp
  - s --src izvorišna IP adresa
  - d --dst odredišna IP adresa, na primjer 10.1.2.3 ili 10.2.3.0/24
  - i --in-interface dolazno sučelje, na primjer eth0
  - o --out-interface odlazno sučelje
- uzorci za protokole UDP i TCP (-p udp ili -p tcp)
  - sport --source-port izvorišni port
  - dport --destination-port odredišni port
- uzorci za protokol ICMP (-p icmp)
  - icmp-type tip icmp poruke, na primjer „echo request”: --icmp-type 8
- stanje konekcije:
  - m state ESTABLISHED, RELATED
  - m conntrack --ctstate ESTABLISHED, RELATED

# Primjeri korištenja



```
firewall# iptables -L -v
```

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

```
firewall# iptables -P INPUT DROP
```

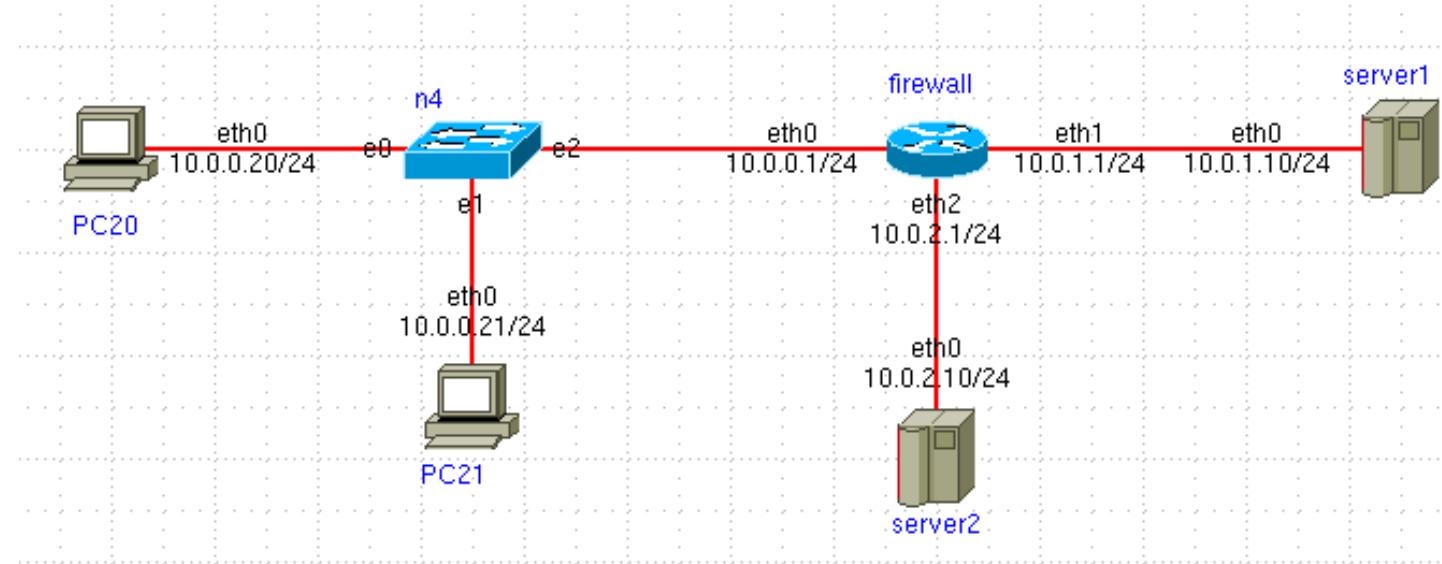
```
firewall# iptables -P OUTPUT DROP
```

```
firewall# iptables -P FORWARD DROP
```

# Primjeri korištenja

PC20# ssh 10.0.1.10

→ ne prolazi, na eth0@firewall  
dolazi SYN ali ga firewall ne propušta.



# iptables -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT

PC20# ssh 10.0.1.10

→ i dalje ne prolazi, na server1 dolazi SYN, on vraća SYN+ACK ali firewall to ne propušta (paket se vidi na eth1@firewall)

# iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

PC20# ssh 10.0.1.10                    ← prolazi jer je “established”

The authenticity of host '10.0.1.10 (10.0.1.10)' can't be established.

# Primjeri korištenja

```
# iptables -A FORWARD -p icmp \
-s 10.0.1.10 -j ACCEPT
```

# himage server1 ping 10.0.0.20

64 bytes from 10.0.0.20: icmp\_seq=34 ttl=63 time=0.269 ms

→ Prolazi i odgovor jer je “established”!

# himage PC20 ping 10.0.1.10

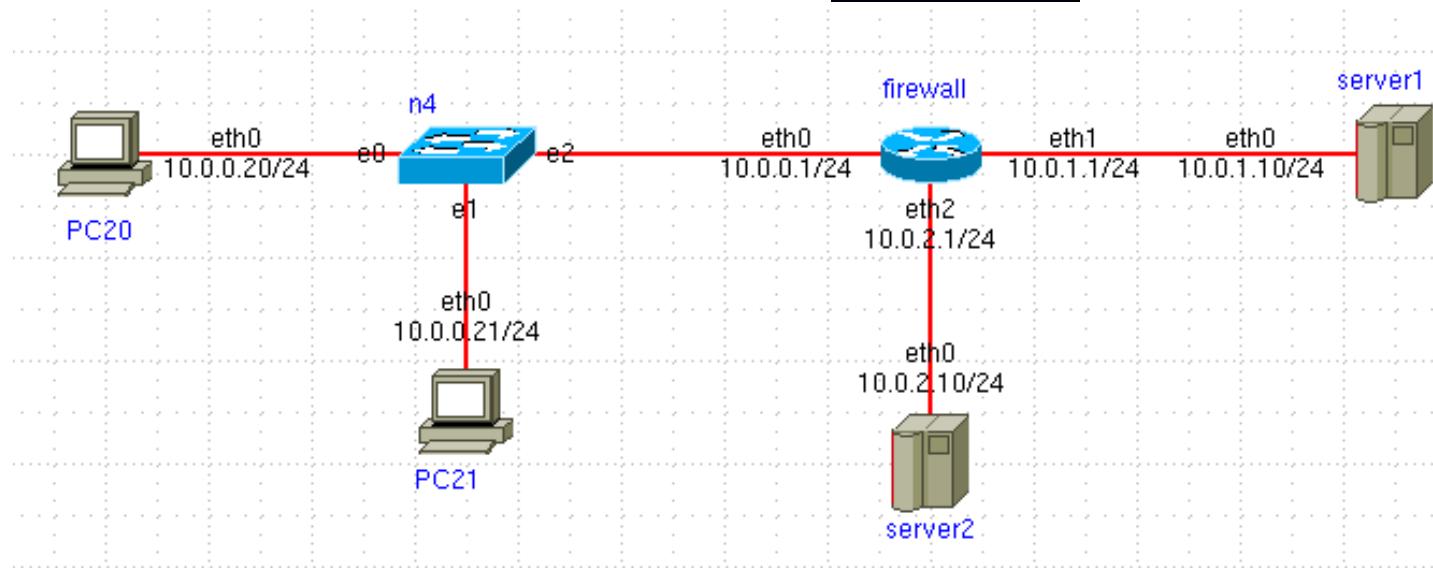
→ ne prolazi jer nije “established”!

# himage server2 nc -u -l -p 1234

```
# iptables -A FORWARD -p udp -d 10.0.2.10 --dport 1234 -j ACCEPT
```

# himage PC20 nc -u 10.0.2.10 1234

→ prolazi (“established”!)



# iptables – jednostavan primjer

```
#!/bin/sh
cmd="/sbin/iptables"

$cmd -P INPUT DROP    # default policy
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP

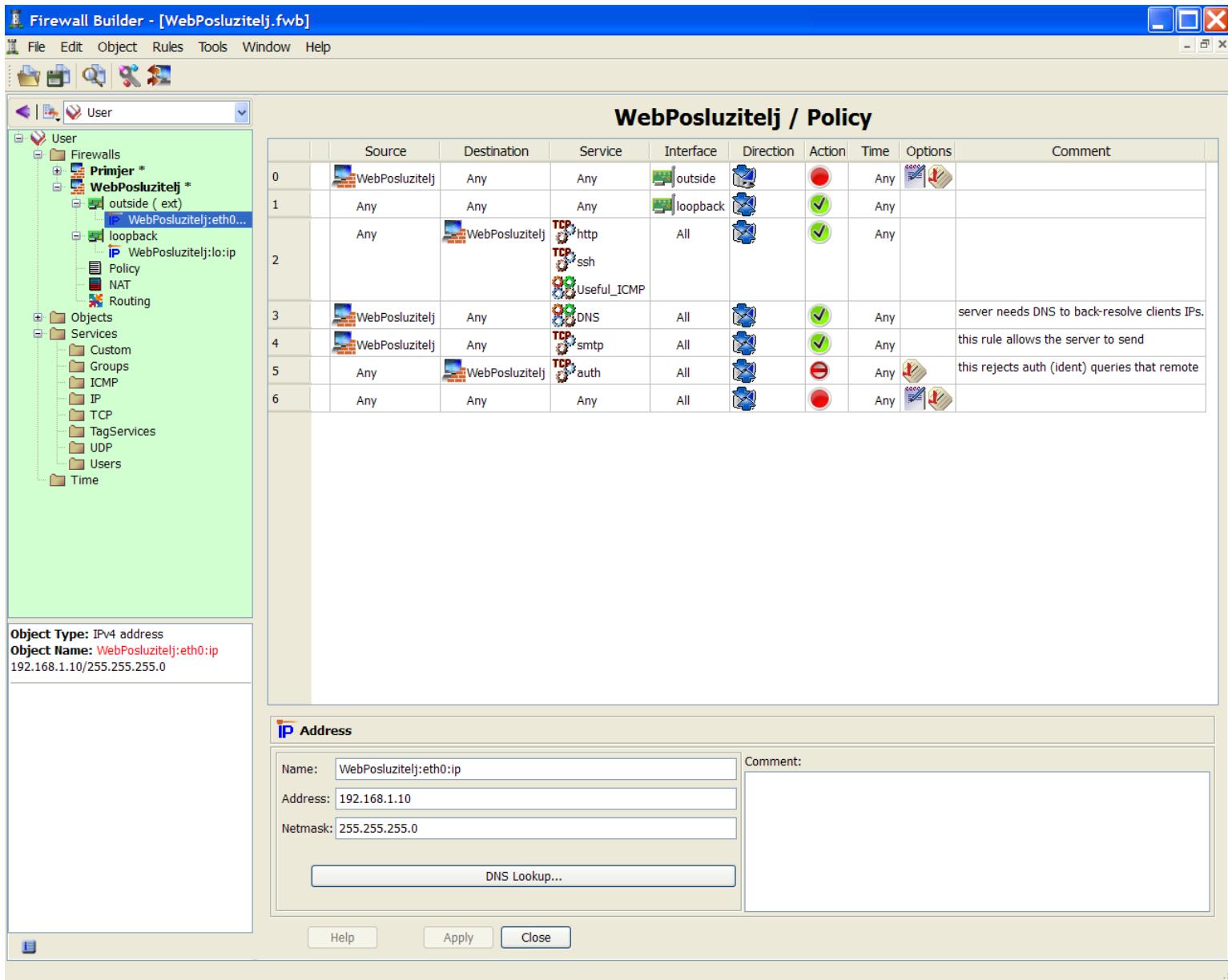
$cmd -F INPUT          # obriše sva pravila
$cmd -F OUTPUT
$cmd -F FORWARD

$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

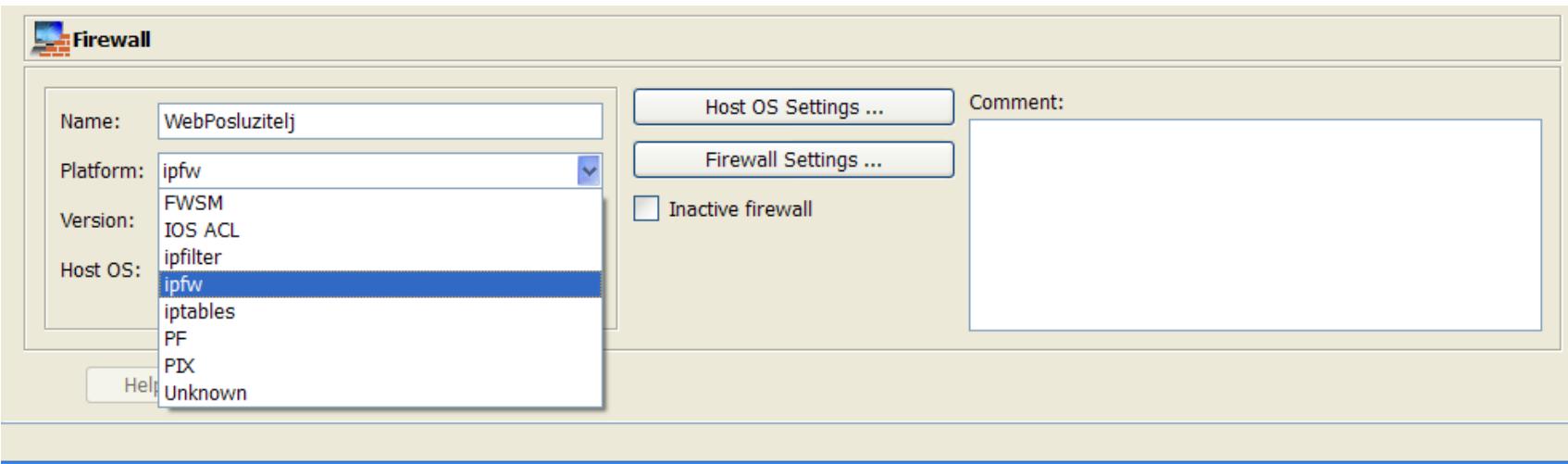
$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
$cmd -A FORWARD -p tcp -s 10.0.0.21 -d 10.0.1.10 \
    -m multiport --dports 21,22,23,25 -j ACCEPT
$cmd -A FORWARD -p icmp -s 10.0.1.10 -j ACCEPT

$cmd -A INPUT -p tcp -s 10.0.0.21 --dport ssh -j ACCEPT
```

# Primjer – Firewall Builder



# Primjer – Firewall Builder



```
cmd="/sbin/iptables"
$cmd -P INPUT    DROP          $cmd -F INPUT
$cmd -P OUTPUT   DROP          $cmd -F OUTPUT
$cmd -P FORWARD  DROP          $cmd -F FORWARD

# accept established sessions
$cmd -A INPUT    -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT   -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD  -m state --state ESTABLISHED,RELATED -j ACCEPT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside			Any		
Any	Any	Any	loopback			Any		
Any	WebPosluzitelj	TCP http TCP ssh TCP Useful_ICMP	All			Any		
WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	out	reject	Any	script	
Any	Any	Any	loopback	in	allow	Any		
Any	WebPosluzitelj	TCP http	All	out	allow	Any		
		TCP ssh						
		Useful_ICMP						
WebPosluzitelj	Any	DNS	All	out	allow	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	out	allow	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	out	reject	Any	script	this rejects auth (ident) queries that remote
Any	Any	Any	All	out	reject	Any	script	

# Rule 0 (eth0 je vanjsko sučelje)

#

\$cmd -A INPUT -i eth0 -s 192.168.1.10 -j DROP

\$cmd -A FORWARD -i eth0 -s 192.168.1.10 -j DROP

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	out	reject	Any	tcp http	
Any	Any	Any	loopback	in	accept	Any		
Any	WebPosluzitelj	TCP http TCP ssh TCP Useful_ICMP	All	in	accept	Any		
WebPosluzitelj	Any	DNS	All	in	accept	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	in	accept	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	in	reject	Any	tcp ident	this rejects auth (ident) queries that remote
Any	Any	Any	All	in	reject	Any	tcp http	

# Rule 1 (loopback sučelje)

#

\$cmd -A INPUT -i lo -j ACCEPT

\$cmd -A OUTPUT -o lo -j ACCEPT

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	outgoing	reject	Any	script	
Any	Any	Any	loopback	outgoing	accept	Any		
Any	WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All	outgoing	accept	Any		
WebPosluzitelj	Any	DNS	All	outgoing	accept	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	outgoing	accept	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	outgoing	reject	Any	script	this rejects auth (ident) queries that remote
Any	Any	Any	All	outgoing	reject	Any	script	

# Rule 2 (global) (1. dio)

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 3 \
          -m state --state NEW -j ACCEPT
$cmd -A INPUT -p icmp -m icmp --icmp-type 0/0 \
          -m state --state NEW -j ACCEPT
$cmd -A INPUT -p icmp -m icmp --icmp-type 11/0 \
          -m state --state NEW -j ACCEPT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	in	reject	Any	tcp,udp,icmp	
Any	Any	Any	loopback	in	accept	Any		
Any	WebPosluzitelj	TCP http TCP ssh TCP Useful_ICMP	All	out	accept	Any		
WebPosluzitelj	Any	DNS	All	in	accept	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	in	accept	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	in	reject	Any	tcp,udp,icmp	this rejects auth (ident) queries that remote
Any	Any	Any	All	in	reject	Any	tcp,udp,icmp	

# Rule 2 (global) (2. dio)

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 11/1 \
      -m state --state NEW -j ACCEPT
```

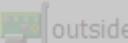
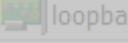
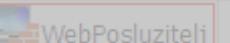
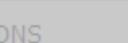
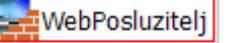
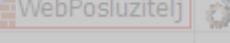
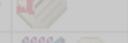
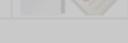
```
$cmd -A INPUT -p tcp -m tcp -m multiport \
      --dports 80,22 -m state --state NEW -j ACCEPT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	out	reject	Any	tcp udp	
Any	Any	Any	loopback	in	allow	Any		
Any	WebPosluzitelj	TCP http TCP ssh ICMP Useful_ICMP	All	in	allow	Any		
WebPosluzitelj	Any	DNS	All	out	allow	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	out	allow	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	in	reject	Any	tcp udp	this rejects auth (ident) queries that remote
Any	Any	Any	All	out	reject	Any	tcp udp	

```
# Rule 3 (global) – serveru treba pristup DNS-u
#
$cmd -A OUTPUT -p tcp -m tcp --dport 53 \
        -m state --state NEW -j ACCEPT
$cmd -A OUTPUT -p udp -m udp --dport 53 \
        -m state --state NEW -j ACCEPT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy									
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment	
 WebPosluzitelj	Any	Any	 outside			Any			
Any	Any	Any	 loopback			Any			
Any	 WebPosluzitelj	TCP http TCP ssh TCP Useful_ICMP	All			Any			
 WebPosluzitelj	Any	 DNS	All			Any		server needs DNS to back-resolve clients IPs.	
 WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send	
Any	 WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote	
Any	Any	Any	All			Any			

```
# Rule 4 (global) - server šalje statistike e-mailom
#
$cmd -A OUTPUT -p tcp -m tcp --dport 25 \
      -m state --state NEW -j ACCEPT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	out	reject	Any	tcp,udp,icmp	
Any	Any	Any	loopback	in	allow	Any		
Any	WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All	in	allow	Any		
WebPosluzitelj	Any	DNS	All	in	allow	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	in	allow	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	in	reject	Any	tcp,udp,icmp	this rejects auth (ident) queries that remote
Any	Any	Any	All	out	reject	Any	tcp,udp,icmp	

```
# Rule 5 (global) – odbaci autentifikacijske zahtjeve (ident)
#
$cmd -A INPUT -p tcp -m tcp --dport 113 -j REJECT
```

# Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside	In	Deny	Any	Log	
Any	Any	Any	loopback	In	Allow	Any		
Any	WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All	In	Allow	Any		
WebPosluzitelj	Any	DNS	All	In	Allow	Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All	In	Allow	Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All	In	Deny	Any	Log	this rejects auth (ident) queries that remote
Any	Any	Any	All	In	Deny	Any	Log	

```
# Rule 6 (global) – zapiši sve ostale pakete
$cmd -N RULE_6
$cmd -A OUTPUT -j RULE_6
$cmd -A INPUT -j RULE_6
$cmd -A RULE_6 -j LOG --log-level info \
                  --log-prefix "RULE 6 -- DENY "
$cmd -A RULE_6 -j DROP
```

# NAT - Network Address Translation

- RFC 3022
- pretvorba privatnih IP adresa (iz privatne mreže) u globalno jedinstvene javne IP adrese
  - više računala iz privatne mreže pristupa Internetu korištenjem jedne javne IP adrese (ili nekoliko adresi)
- NAT je u osnovi *proxy* – jedan host šalje zahtjeve u ime svih internih računala
  - implementiran na transportnom sloju
- informacije skrivene u podacima (na višim slojevima) se ne mijenjaju – moguće iskorištavanje slabosti sustava
- načini rada:
  - statička translacija
  - dinamička translacija
  - translacija s balansiranjem opterećenja
  - “*network redundancy translation*”

# NAT

- statička translacija
  - koristi se kad postojeći resursi unutar privatne mreže moraju biti javno dostupni
  - preslikava područje javnih IP adresa u blok iste veličine s privatnim adresama
    - primjer: 161.53.19.0–161.53.19.255 ↞ 10.1.2.0–10.1.2.255.
  - jednostavna statička translacija za svaku korištenu IP adresu
- “port forwarding”
  - tip statičke translacije u kojem se proslijeđuje promet za samo određeni port a ne za cijelu IP adresu
  - primjer: e-mail poslužitelj je na 10.1.1.21, a vanjska IP adresa na NAT uređaju je 161.53.19.200
    - statičko preslikavanje 161.53.19.200:25 na 10.1.1.21:25
  - može se uspostaviti puno različitih usluga na jednoj IP adresi
    - posluživanje se može obavljati na više računala u internoj mreži

# NAT

- dinamička translacija
  - naziva se još “overloading”, NAPT (Network Address and Port Translation) i “single address NAT”
  - veća grupa internih klijenata dijeli jednu IP adresu (ili malu grupu internih IP adresa) u svrhu skrivanja identiteta ili proširivanja prostora raspoloživih mrežnih adresa
  - portovi na jednoj javnoj IP adresi mogu se proslijediti na specificirane privatne IP adrese
  - translacija se kreira tek kad unutarnji klijent uspostavlja konekciju kroz NAT
    - vanjska računala ne mogu nikako adresirati unutarnja računala koja su “zaštićena” korištenjem dinamički translatiranih IP adresa.
    - tehnički je moguće koristiti IP “source-routing” za usmjeravanje kroz NAT ali svi NAT uređaji takve pakete odbacuju!

# NAT

- balansiranje opterećenja
  - balansiranje opterećenja poslužitelja korištenjem statičkog NAT
  - slično dinamičkoj translaciji ali u drugom smjeru
  - FW odabire kojem od poslužitelja (iz poola) treba proslijediti zahtjev
  - radi sa stateless protokolima ili protokolima koji održavaju stanje na klijentu
- mrežna redundancija
  - balansiranje opterećenja linkova prema ISP
  - automatsko prebacivanje na drugi link
  - radi s dinamičkom translacijom na isti način kao što balansiranje opterećenja radi sa statičkom translacijom
  - FW povezan na više ISP-ova
    - svako (vanjsko) sučelje ima javnu adresu
    - interna adresa je jedinstvena
  - za svaku konekciju određuje preko koje mreže treba ostvariti vezu
    - na temelju opterećenja linkova
    - linkovi koji ne rade tretiraju se kao potpuno opterećeni linkovi

# Problemi s NAT-om

- neki protokoli ne rade ispravno kad se promijeni broj porta
- nekoliko protokola ne može se koristiti uz (standardni) NAT jer:
  - zahtijevaju otvaranje povratnog kanala prema klijentu (H.323 video telekonferencije)
  - informacije o TCP/IP adresi sadržane su u protokolima na višim slojevima (FTP)
  - TCP zaglavlje je šifrirano (PPTP i IPSec AH - fw mora biti krajnja točka)
  - koriste originalne IP adrese iz razloga sigurnosti
- napredniji FW može analizirati odlazne konekcije tih protokola i uspostaviti translacije koje će čekati odgovor
  - ili se koriste specifični posrednički programi (*proxy*) u kombinaciji s NAT mehanizmima
- teoretski najviše 65,536 konekcija na jednoj IP adresi
  - u pravilu ograničeno na < 50,000 konekcija (portovi rezervirani za druge namjene)
  - na Linuxu standardno omogućeno korištenje 4096 portova

# Sigurnost?

- NAT skriva klijente te ih nije moguće hakirati. → Ne! Moguće je!
  - statička translacija ne štiti unutarnja računala
    - zamjenjuje informacije o portovima jedan-na-jedan te se i napadi translatiraju kao i regularni zahtjevi
  - ako klijent uspostavi konekciju postoji i povratna veza
  - ako se konekcija može presretati ili je podložna napadu “*man-in-the-middle*” tada je “*man-in-the-middle*” krajnja točka.
  - loša implementacija omogućava “provalu” na NAT
  - *Source routing*
    - upiše se cijeli puta do odredišta
    - NAT uređaj se upiše kao jedna od adresa
    - NAT usmjerava datagram do krajnjeg odredišta
    - FW/NAT obavezno mora odbacivati takve datagrame

# Sigurnost?

- prijevara s internog računala
  - korisnik iz neznanja ili nepažnje pročita falsificirani e-mail s linkom na web stranicu ili posjeti “opasne web stranice” te učita softver koji skriva Trojanskog konja
  - rješenje je u primjeni aplikacijski specifičnih posrednika
    - rade na visokom sloju
    - provjeravaju sadržaj koji protokol razmjenjuje (na primjer u HTTP protokolu traže sumnjive sadržaje: Java applet, ActiveX kontrole, izvršni programi, ...)
- problem vremenskih kontrola tablice stanja
  - FW se ne može pouzdati na informacije o zatvaranju sesije
    - mnogi protokoli nemaju očigledan završetak
    - vremenske kontrole mogu znatno varirati i u pravilu nisu objavljene
  - prije isteka vremenske kontrole postojeća konekcija se može zloupotrijebiti
    - uz poznavanje točne IP adrese i porta te originalne IP adrese

# Posrednički poslužitelji

- Vatrozid radi na 3. sloju ISO/OSI RM-a (i 4. sloju)
  - Problematično za protokole koji vrše nekakva multipleksiranja
  - Primjer protokola HTTP, virtualnih poslužitelja i URL-ova
- Posrednički poslužitelji omogućavaju bolji nadzor mrežnog prometa
  - Moguća detekcija zločudnog koda
  - Crne i bijele liste
  - Bilježenje pristupa radi rektroaktivne analize
  - Dodatno, mreža je efikasnija
- ALI: Bez vatrozida nije moguće dosljedno provoditi politiku korištenja posredničkog poslužitelja

# Sustavi za detekciju upada (1)

- engl. Intrusion Detection Systems
- Temelje se na ideji da se praćenjem ponašanja sustava ili prometa na mreži može detektirati incident
- Podjele prema načinu rada
  - Bazirane na pravilima
  - Na detekciji ponašanja ili anomalijama
- Podjele prema mjestu nadzora
  - Mrežni (NIDS) – uzimaju podatke s mreže
  - Računalni sustavi (HIDS) – uzimaju podatke s računala

# Sustavi za detekciju upada (2)

- Mrežni sustavi
  - Postavljaju se na neke ključne točke na kojima snimaju promet
    - Bitno je da vide promet mrežnog segmenta kojeg želimo pratiti
  - Mogući problemi s brzinama (10G+)
  - Problem je i šifrirana komunikacija
- Mnoštvo različitih sustava na tržištu
  - Popularna implementacija otvorenog koda - SNORT, BRO, OSSEC, Suricata

# Sustavi za prevenciju upada

- Osim detekcije rade i prevenciju
  - Intrusion Prevention Systems (IPS)
- Prevencija može biti postavljanje dodatnih pravila na vatrozidu
  - Pravila privremena ili stalna
- Ako nisu dobro podešeni mogu onemogućiti ispravan rad mreže!

# Otkrivanje ranjivosti u mreži

- Ranjivosti u računalnoj mreži su neizbjježne(!)
  - Treba ih što prije otkriti i ukloniti
- Otkrivanje ranjivosti može se obaviti na dva temelja načina
  - Skeniranje mrežnih raspona
    - Nessus, OpenVAS
    - Jednostavno, ali opterećuje mrežu i puno lažno točnih detekcija
    - Jeftina, ali ne otkrivaju nužno sve ranjivosti
  - Penetracijska ispitivanja
    - Obavljuju pojedinci ili timovi koji traže ranjivosti
    - Cilj je i pokušati iskoristiti ranjivost, ne samo ju naći
    - Skuplja od skeniranja
    - Ne otkrivaju nužno sve ranjivosti

# *Honeypot*

- mamac (engl. honeypot) je nekakvo računalo ili računalni resurs čija isključiva namjena je da bude iskorišten ili manipuliran na nekakav način
  - mamac može biti računalo, usluga, podatak
- ideja je na mrežu staviti računala i usluge koje nitko ne koristi i potom pratiti kada im netko pristupa
  - pristup znači nedozvoljenu aktivnost!
- podjela
  - visoke interakcije (cijelo računalo) ili niske interakcije (samo pojedina usluga, možda ne u cijelosti)



SVEUČILIŠTE U ZAGREBU



Diplomski studij

# Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost elektroničke pošte



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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/>.

# Incidenti vezani uz elektroničku poštu

- 4 vrste sigurnosnih incidenata
  - neprikladno ponašanje koje nije specifično samo za elektroničku poštu
    - prijetnje, otkrivanje povjerljivih informacija, prevare
  - zlonamjerne poruke s neželjenim posljedicama po računalo korisnika
    - virusi, crvi...
  - zloupotreba usluge
    - spam, hoax
    - društveni inžinjering
  - gubitak privatnosti i anonimnosti
    - web bug
    - kompromitiranje poruka u mreži

# Gubitak privatnosti i anonimnosti

- web bug
  - klijent elektroničke pošte prikazuje HTML
  - pošiljatelj može uključiti link na sliku koja kontaktira njegov web-poslužitelj
  - “tko je pročitao mail?”
- kompromitacija poruke
  - *store-and-forward*
  - poruke prolaze kroz niz mail-poslužitelja – vide je svi na putu
  - rješenja:
    - zahvati u infrastrukturi sustava, mreže, usmjeravanja
    - šifriranje s kraja na kraj
      - S/MIME
      - PGP

# Simple Mail Transfer Protocol

- definiran je 1982. godine u RFC 821 → RFC 2821 →RFC 5321
- specificira način prijenosa poruka između dva računala
  - ne ovisi o mrežnom protokolu
  - omogućuje prosljeđivanje poruka kroz raznovrsne mreže
- strogo definira sintaksu i redoslijed odvijanja transakcije
  - koristi retke teksta za razmjenu informacija
  - polazno računalo šalje SMTP naredbe, na koje ciljno računalo odgovara kodovima koji mogu označavati uspjeh ili pogrešku
  - svaka naredba pošiljatelja mora dobiti odgovor primatelja
- naredbe
  - obavezne: HELO, MAIL, RCPT, DATA, RSET, VRFY, NOOP, QUIT
  - neobavezne: SEND, SOML, SAML, EXPN, HELP, TURN
- čvorovi
  - MUA (*Mail User Agent*)
  - MTA (*Mail Transfer Agent*)

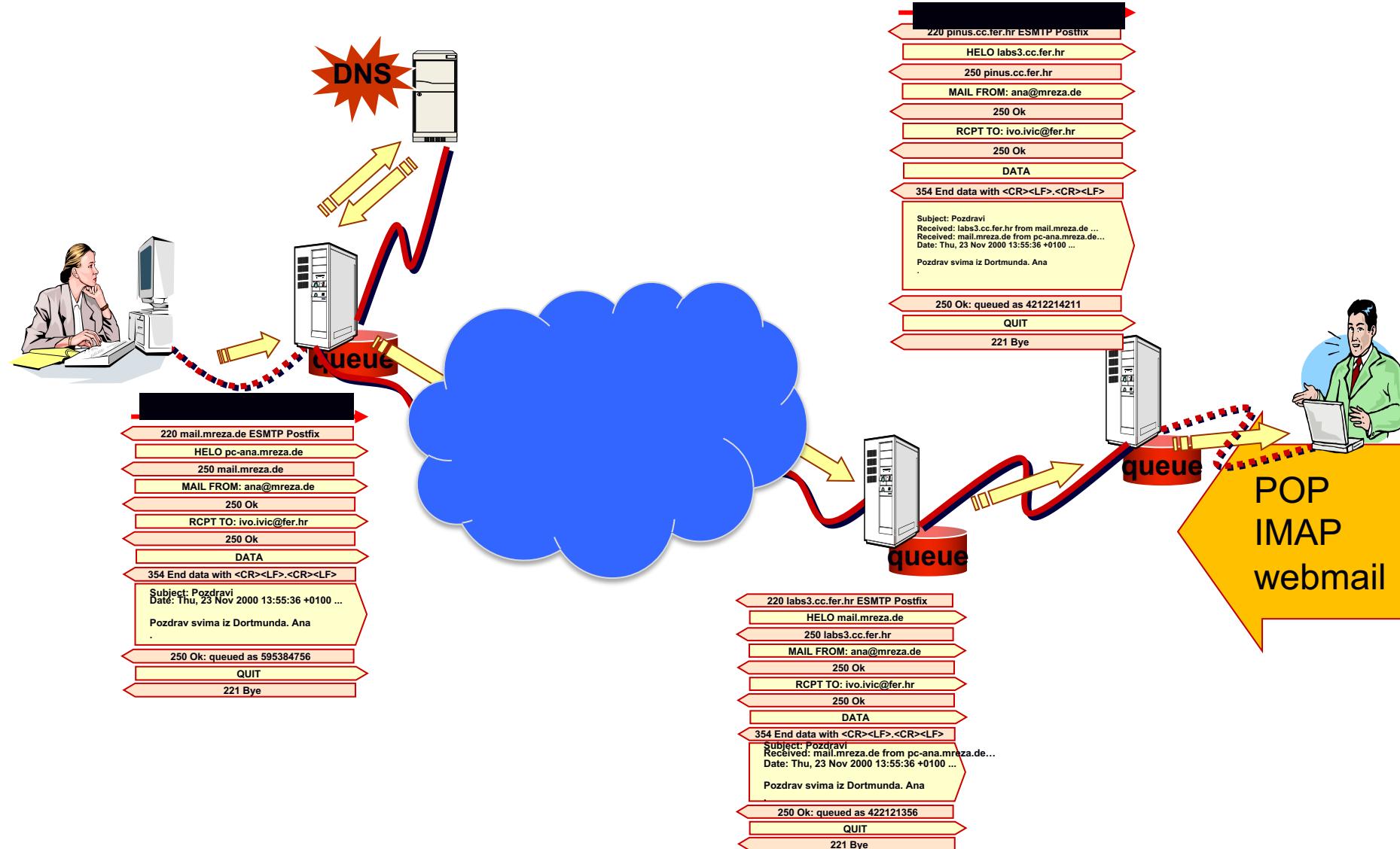
# Simple Mail Transfer Protocol - primjer

```
dave@Mint ~ $ telnet 192.168.254.167 25
Trying 192.168.254.167...
Connected to 192.168.254.167.
Escape character is '^]'.
220 smtp-sink ESMTP
HELO localhost
250 smtp-sink
MAIL FROM: sender@domain.com
250 2.1.0 Ok
RCPT TO: recipient@domain.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: This is the subject!
This is the test message body of this email!
.
250 2.0.0 Ok
Quit
221 Bye
Connection closed by foreign host.
```

slika preuzeta: <http://dfirdave.blogspot.com/>

više na: <http://www.yuki-onna.co.uk/email/smtp.html>

# Mehanizam slanja elektroničke pošte



# SMTP – komunikacija MUA i MTA

ana@mreza.de



pc-ana.mreza.de

From:  
ana@mreza.de  
To: ivo.ivic@fer.hr  
Subject: Pozdravi

Pozdrav svima iz  
Dortmunda.

Ana

uspostavlja vezu spajanjem na port 25

220 mail.mreza.de ESMTP Postfix

HELO pc-ana.mreza.de

250 mail.mreza.de

MAIL FROM: ana@mreza.de

250 Ok

RCPT TO: ivo.ivic@fer.hr

250 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

Subject: Pozdravi  
Date: Thu, 24 Nov 2011 13:55:36 +0100 ...

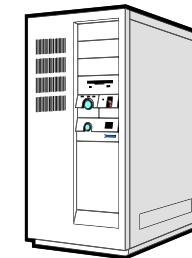
Pozdrav svima iz Dortmundu. Ana.

.

250 Ok: queued as 595384756

QUIT

221 Bye



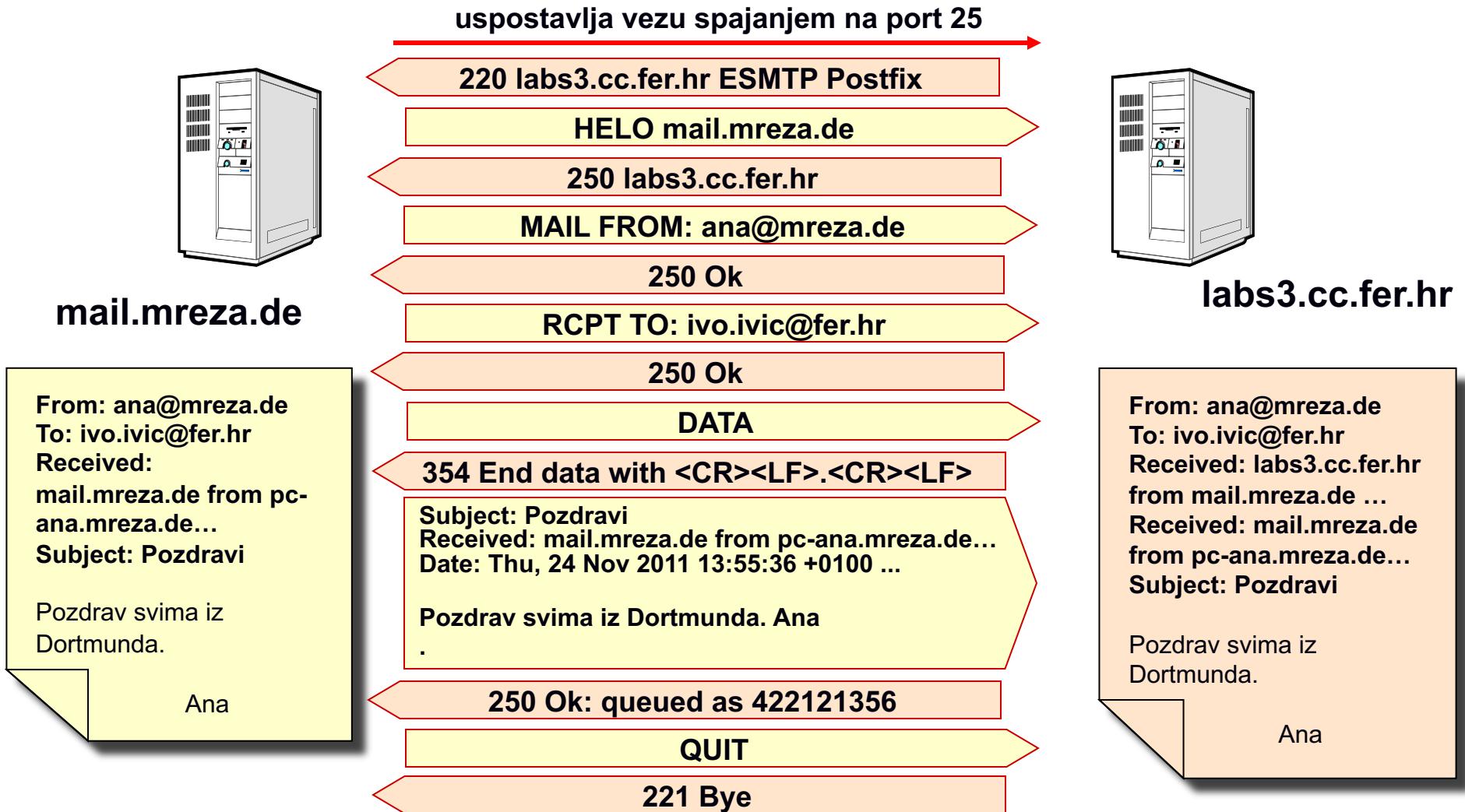
mail.mreza.de

From: ana@mreza.de  
To: ivo.ivic@fer.hr  
Received: mail.mreza.de  
from pc-ana.mreza.de...  
Subject: Pozdravi

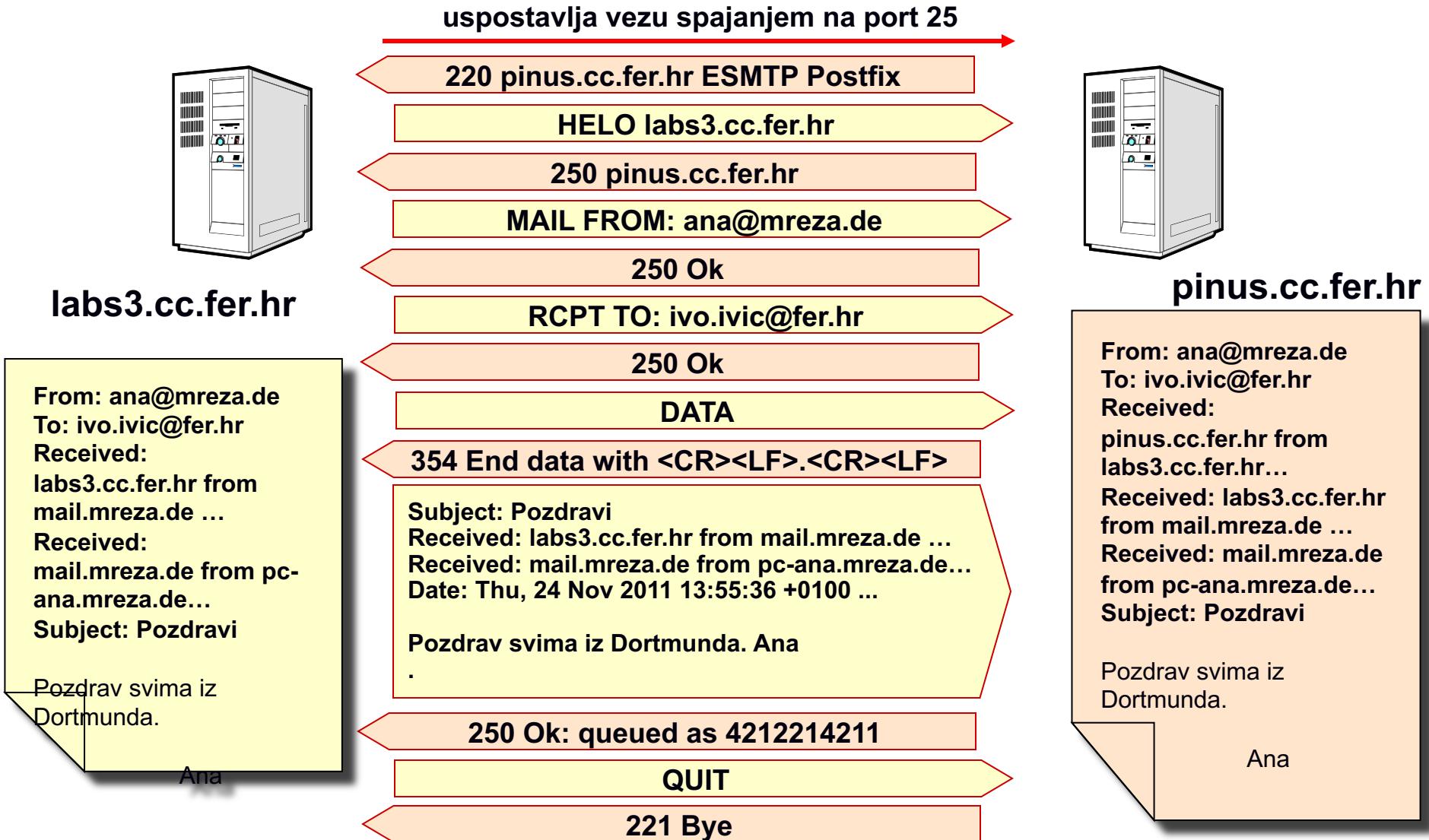
Pozdrav svima iz  
Dortmunda.

Ana

# SMTP – komunikacija MTA i MTA



# SMTP – komunikacija MTA i MTA



# Sigurnosni problemi SMTP-a

- uopće **nema** sigurnosnih mehanizama!
- otvoren i u tekstualnom obliku
- nema autentifikacije
- podrazumijeva se povjerenje i suradnja
  - otvoreni mail relay
  - ne provjerava se tko se spaja na poslužitelj
  - prihvaca se pošta za korisnika koji nije na lokalnoj mreži

# Borba protiv neželjene pošte

- autentifikacija i reputacija korisnika
- izazov/odgovor
- zaštitne sume
- crne liste temeljene na DNS-u
- striktno pridržavanje RFC-ova
  - mora se čekati odgovor poslužitelja prije slanja podataka
  - sive liste (privremeno se odbacuje pošta koja stiže od nepoznatih SMTP poslužitelja, generira se greška 4xx)
  - provjera sintakse HELO i EHLO
  - višestruki nedohvatljivi MX-zapisi na DNS-u
  - detekcija raskida veze naredbom QUIT
- honeypot
- prepoznavanje uzorka...

# Moguća rješenja problema sigurnosti

- provjera IP adrese klijenta
    - pristup moguć samo onima na popisu
  - ograničena upotreba nekih naredbi
    - nakon autentifikacije
  - ograničena upotreba naredbi za pristup do korisničkih adresa
    - EXPN, VRFY – je li adresa ili lista valjana? - SPAM!
  - provjera valjanosti podataka u zaglavljima
    - envelope, MAIL From:
  - ograničenje veličine poruke
  - ograničenje broja poruka u zadanom vremenu
  - vođenje logova
- 
- većina ovih rješenja **nisu dio standarda SMTP**

# Autentifikacija korisnika

- POP-before-SMTP ili SMTP-after-POP
  - poruke je moguće slati tek nakon “dokaza” da ih se može i preuzeti
- **SMTP-AUTH (RFC 2554)** – port 587
  - pregovaranje oko protokola – nove naredbe
- **ESMTP (RFC 5321 + RFC 5336)**
  - Simple Authentication and Security Layer - SASL
- Microsoft: Secure Password Authentication – SPA putem SMTP-AUTH
- ne pomažu u rješavanju spama!
- zamjena SMTP-a nije praktična

# Extended SMTP – ekstenzije

- 8BITMIME — 8-bitni prijenos podataka, RFC 1652
- ATRN — autentificirani TURN za On-Demand Mail Relay, RFC 2645
- SMTP-AUTH — autentificirani SMTP, RFC 4954
- CHUNKING — cjepljanje velikih poruka, RFC 3030
- DSN — obavijest o dostavi, RFC 3461
- ETRN — udaljeni TURN, RFC 1985
- HELP — pomoć, RFC 821
- PIPELINING — slanje više naredbi odjednom, RFC 2920
- SIZE — deklaracija veličine poruke, RFC 1870
- STARTTLS — Transport layer security, RFC 3207
- UTF8SMTP — korištenje UTF-8 u zaglavljima, RFC 5336

# SMTP-AUTH – primjer komunikacije

```
S: 220-smtp.example.com ESMTP Server
C: EHLO client.example.com
S: 250-smtp.example.com Hello client.example.com
S: 250-AUTH GSSAPI DIGEST-MD5
S: 250-ENHANCEDSTATUSCODES
S: 250 STARTTLS
C: STARTTLS
S: 220 Ready to start TLS ... nastavlja se šifrirana
komunikacija...
C: EHLO client.example.com
S: 250-smtp.example.com Hello client.example.com
S: 250 AUTH GSSAPI DIGEST-MD5 PLAIN
C: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=
S: 235 2.7.0 Authentication successful
```

# Mail Relay

\*.dsl.t-com.hr



From: kolinda@predsjednik.hr  
To: trump@whitehouse.gov  
Subject: Pozdravi

Dragi kolega, primite puno pozdrava od ...

uspostavlja vezu spajanjem na port 25

220 mail.tel.fer.hr ESMTP Postfix

HELO gazda.predsjednik.hr

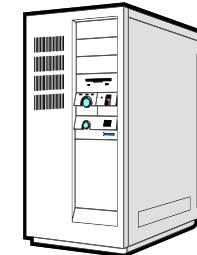
250 mail.tel.fer.hr

MAIL FROM: kolinda@predsjednik.hr

250 Ok

RCPT TO: trump@whitehouse.gov

550 Relaying Denied



mail.tel.fer.hr

mail.tel.fer.hr prihvaca poštu samo:

- od lokalnih korisnika za vanjske korisnike
- od vanjskih korisnika za lokalne korisnike
- od lokalnih korisnika za lokalne korisnike

lokalno: \*@tel.fer.hr



Povjerljivost komunikacije

S/MIME

# Kako osigurati povjerljivost

- s kraja na kraj?
- od čvora do čvora?
- nekoliko raznih rješenja
  - Privacy-enhanced Electronic Mail – PEM (RFC 1421-1424)
    - nije zaživjelo, ovisilo o PKI s jednim korijenom
    - nametanje središnjeg autoriteta
  - Pretty Good Privacy – PGP
    - Web of Trust – PKI
    - OpenPGP, GnuPG
  - proširenja standarda MIME
    - Mime Object Security Services – MOSS (RFC 1848)
    - S/MIME (RFC 5751)

# S/MIME

- sigurnosno proširenje standarda MIME
  - Multipurpose Internet Mail Extension
- nije ograničeno samo na elektroničku poštu!
  - koristi se i za druge protokole – npr. HTTP
- komercijalna primjena i poslovni svijet
  - korisnicima za osobnu upotrebu “bolji” PGP
- povijest:
  - S/MIME v1, 1995. – RSA Security, Inc.
  - S/MIME v2, 3/1998. – informativni RFC 2311 i 2312
  - S/MIME v3, 6/1999. – IETF S/MIME Email Security WG – RFC 2630-2634
    - 9/2009 - RFC 5652 - CMS
    - 1/2010 - RFC 5751 – v3.2

# Usluge kriptozaštite koje nudi S/MIME

- autentifikacija
  - cjelovitost poruke
  - neporecivost
  - privatnost
  - sigurnost podataka
- 
- no, što je MIME?
    - *Multipurpose Internet Mail Extensions*



digitalni potpis



šifriranje

# Zašto je potreban MIME?

- RFC 822 definira format elektroničke poruke
  - kasnije RFC 2822, 5322
- ograničenja formata elektroničke pošte prema RFC 822:
  - prijenos binarnih datoteka (npr. izvršnih)
  - duljina retka 1000 znakova (998 + CR-LF)
  - poruke pisane nacionalnim jezicima (samo 7-bitni ASCII)
  - prijevod iz ASCII u EBCDIC
  - neke implementacije ne drže se specifikacije iz RFC 822
- ograničenja SMTP-a
  - odbijaju se prevelike poruke
  - mijenja, briše ili mijenja raspored CR/LF
  - reže ili cijepa retke duže od 76 znakova
  - miče tabove i razmake na kraju retka ili poruke
  - dopunjava retke da budu iste veličine
  - pretvara tab u razmake

# Standard MIME

- omogućuje:
  - korištenje svih znakova, uključivo i 2-oktetne znakove (istočnjačka pisma)
  - definiranje strukture poruke i vrste poruke
  - dodavanje jedne ili više binarnih, HTML ili višemedijskih datoteka u poruku (paziti na duljinu takvih poruka – RFC 1870)
  - nije u konfliktu sa specifikacijama u RFC 821 i 822
  - neki dijelovi standarda MIME mogu se koristiti i za druge primjene (HTTP)
- jedini zahtjev
  - klijent mora biti kompatibilan sa standardom

# Korištenje standarda MIME

- uvodi se 5 novih polja u zaglavlje poruke
  - daju dodatnu informaciju o tijelu
- definirani su formati sadržaja
  - standardizira se reprezentacija sadržaja i daje podrška za višemedijske poruke
- definiraju se metode kodiranja pri prijenosu
  - čuvaju sadržaj od mogućih promjena tijekom prijenosa
- MIME standardizira način na koji se upravlja informacijama i sadržajem u višemedijskoj okolini

# Nova zaglavlja

- MIME-Version [**MIME-Version: 1.0**]
  - verzija MIME standarda, trenutno samo 1.0 (RFC 2045, 2046)
- Content-Type [**Content-Type: text/plain; charset=UTF-8**]
  - opisuje vrstu podataka u pojedinom MIME entitetu (tip i podtip)
- Content-Transfer-Encoding [**Content-Transfer-Encoding: quoted-printable**]
  - definira način kodiranja podataka u MIME poruci
- Content-ID [**Content-ID: <E796FD66-8942-41B1-9C78-BAA583C156FD>**]
  - jednoznačno definira MIME entitet, slično kao Message-ID: poruku
- Content-Description [**Content-Description: slicica**]
- dodatno Content-Disposition [**Content-Disposition: attachment; filename="file.pdf"**]
  - definira kako treba tretirati MIME entitet, kao dio poruke (inline) ili vanjski dodatak (attachment), tek od RFC 2183

# Primjer zaglavlja MIME

...

```
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
    boundary="-----_NextPart_000_002F_01C1C57E.29CC71A0"
```

This is a multi-part message in MIME format.

```
-----_NextPart_000_002F_01C1C57E.29CC71A0  
Content-Type: multipart/alternative;  
    boundary="-----_NextPart_001_0030_01C1C57E.29CC71A0"
```

```
-----_NextPart_001_0030_01C1C57E.29CC71A0  
Content-Type: text/plain;  
    charset="iso-8859-2"  
Content-Transfer-Encoding: quoted-printable  
...
```

# Content-Type: tipovi i podtipovi podataka

Tip	Podtip	Content-Type
Text	Plain, enriched, html	text/plain, text/enriched, text/html
Image	Jpeg, tiff, gif	image/jpeg, image/tiff, image/gif
Audio	Basic, mpeg	audio/basic, audio/mpeg
Video	Mpeg, quicktime	video/mpeg, video/quicktime
Application	Octet-stream, postscript, pdf, zip, msword	application/pdf, application/zip
Message	Rfc822, partial, external-body	message/rfc822, message/partial
Multipart	Mixed, alternative, digest, parallel	multipart/mixed, multipart/digest

# Multipart

- omogućuje da se u tijelu jedne poruke šalje više MIME entiteta
- dijelovi su odvojeni graničnim nizom znakova koji je definiran u zaglavlju glavne poruke

```
Content-Type: multipart/mixed; boundary=zxf918
```

This is a MIME-encapsulated message.

--zxf918

Body part1

--zxf918

Body part2

--zxf918--



# Content-Transfer-Encoding

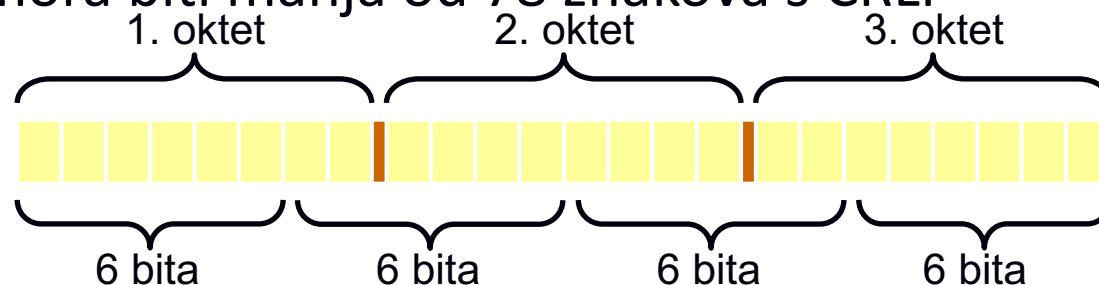
- 7bit
  - poruka se sastoji od linija ne dužih od 998 okteta 7-bitnih podataka, koji završavaju s CRLF
- 8bit
  - poruka se sastoji od linija ne dužih od 998 znakova, koji završavaju s CRLF
- binary
  - poruka se sastoji od niza 8-bitnih znakova bez ograničenja na duljinu linije ili dozvoljene znakove
- quoted-printable
  - uglavnom ASCII, prepoznatljivo
- base64
  - ASCII, neprepoznatljivo

# Content-Transfer-Encoding: quoted-printable

- ako su podaci koji se kodiraju većinom 7-bitni ASCII znakovi, kodirani oblik ostaje većinom razumljiv čitateljima
  - svaki posebni znak može se zamijeniti s odgovarajućim dvoznamenkastim heksadecimalnim ekvivalentom tako da se ispred njega doda znak “=”
  - linije ne smiju biti dulje od 76 znakova (+ CRLF)
- kompromis između čitljivosti, učinkovitosti i robustnosti
- nije striktno definiran i postoje odstupanja u izvedbama
- Elektronička pošta -> Elektroni=C4=8Dka po=C5=A1ta

# Content-Transfer-Encoding: base64

- Content-Transfer-Encoding: base64
  - koristi se podskup US-ASCII (7-bitnih) znakova koji sadrži 65 znakova
  - grupe od 3 okteta kodiraju se u 4 znaka (svaki znak 6 bitova)
  - duljina linije mora biti manja od 78 znakova s CRLF



GIF89 (71 73 70 56 57 : decimal)							
01000111 01001001 01000110 00111000 00111001 (Octet stream)							
010001 110100 100101 000110 001110 000011 1001							
010001 110100 100101 000110 001110 000011 100100							
17	52	37	6	14	3	36	
R	0	1	G	O	D	K	
R01GODK=							

# "Non ASCII" znakovi u zaglavljima

- postoje tehnike kojima se omogućuje kodiranje ne-ASCII teksta u zaglavljima prema RFC 822
- =?charset?encoding?text?=
  - charset: us-ascii, iso8859-1 do iso8859-9
  - encoding: B ili Q
    - Q: inačica quoted-printable kodiranja, space se kodira s \_
    - B: kodiranje prema base64
  - text: niz ASCII znakova koji se podvrgava pravilima kodiranja
- kodirana riječ ograničena je na 75 znakova
  - From: =?iso-8859-2?Q?Alen\_Ba=BEant?= <alen.bazant@fer.hr>
  - From: =?iso-8859-2?Q?Martina\_Jel=E8i=E6?= <martina.jelcic@fer.hr>
  - Subject: =?euc-kr?B?x9Gx28GmuPEgKE1JTUUgdGVzdCk=?=

# Zaključno o standardu MIME

- neizbježan pri prijenosu podataka Internetom
- objektno-orientirana struktura poruke po standardu MIME omogućuje mu da bude višenamjenski standard
- primjenom standarda MIME moguće je prenositi poruke između sustava koji koriste različite formate

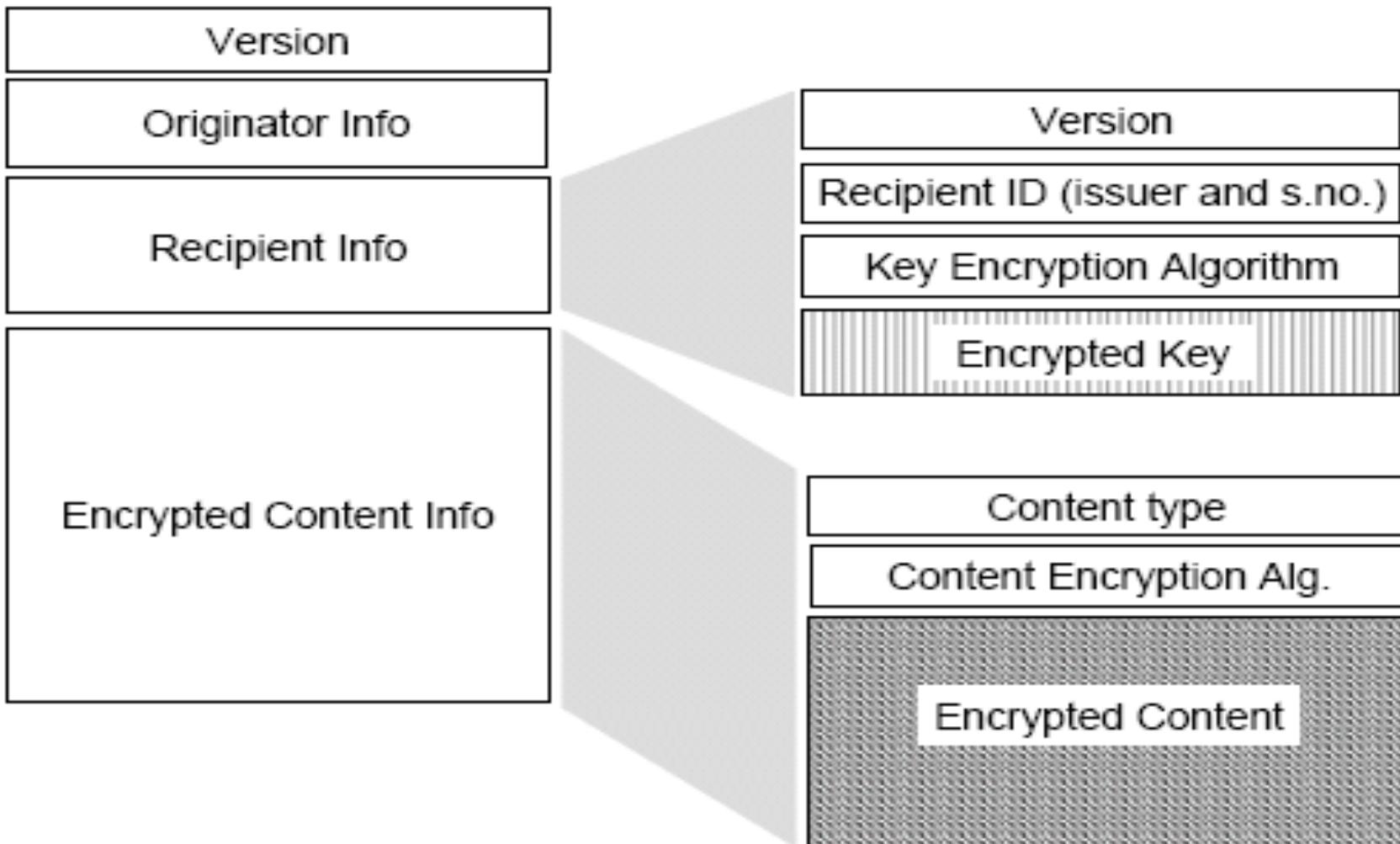
# Cryptographic Message Syntax

- S/MIME se temelji na Cryptographic Message Syntax (CMS)
  - RFC 5652 (ali i RFC 5911 – ASN.1)
  - standard IETF-a za prijenos šifriranih poruka
  - digitalni potpis, sažetak, autenfitikacija, šifriranje bilo kojeg oblika podataka
  - temeljen na sintaksi standarda RSA Security (PKCS#7)
- arhitektura temeljena na upravljanju ključevima i certifikatima

# Funkcije: *enveloped-data*

- šifrirani sadržaj bilo kojeg tipa i šifrirani ključevi za jednog ili više korisnika
  - digitalna ovojnica
- način rada:
  - stvara se jednokratni ključ za šifriranje za RC2/40 ili DES
  - taj se ključ šifrira za svakog primatelja njegovim javnim ključem
  - sve potrebne informacije (certifikat pošiljatelja, algoritam, šifrirani ključ) pohrane se u vrijednost *RecipientInfo*
  - sadržaj se šifrira jednokratnim ključem za šifriranje (moguće uz *padding*)
  - vrijednosti *RecipientInfo* za sve primatelje prikupe se i uz šifrirani sadržaj postave u vrijednost *EnvelopedData*
- funkcija osigurava privatnost i sigurnost podataka

# *Enveloped data*



# Primjer šifrirane poruke

Content-Type: application/pkcs7-mime;  
smime-type=enveloped-data;  
name=smime.p7m

Content-Transfer-Encoding: base64  
Content-Disposition: attachment;  
filename=smime.p7m

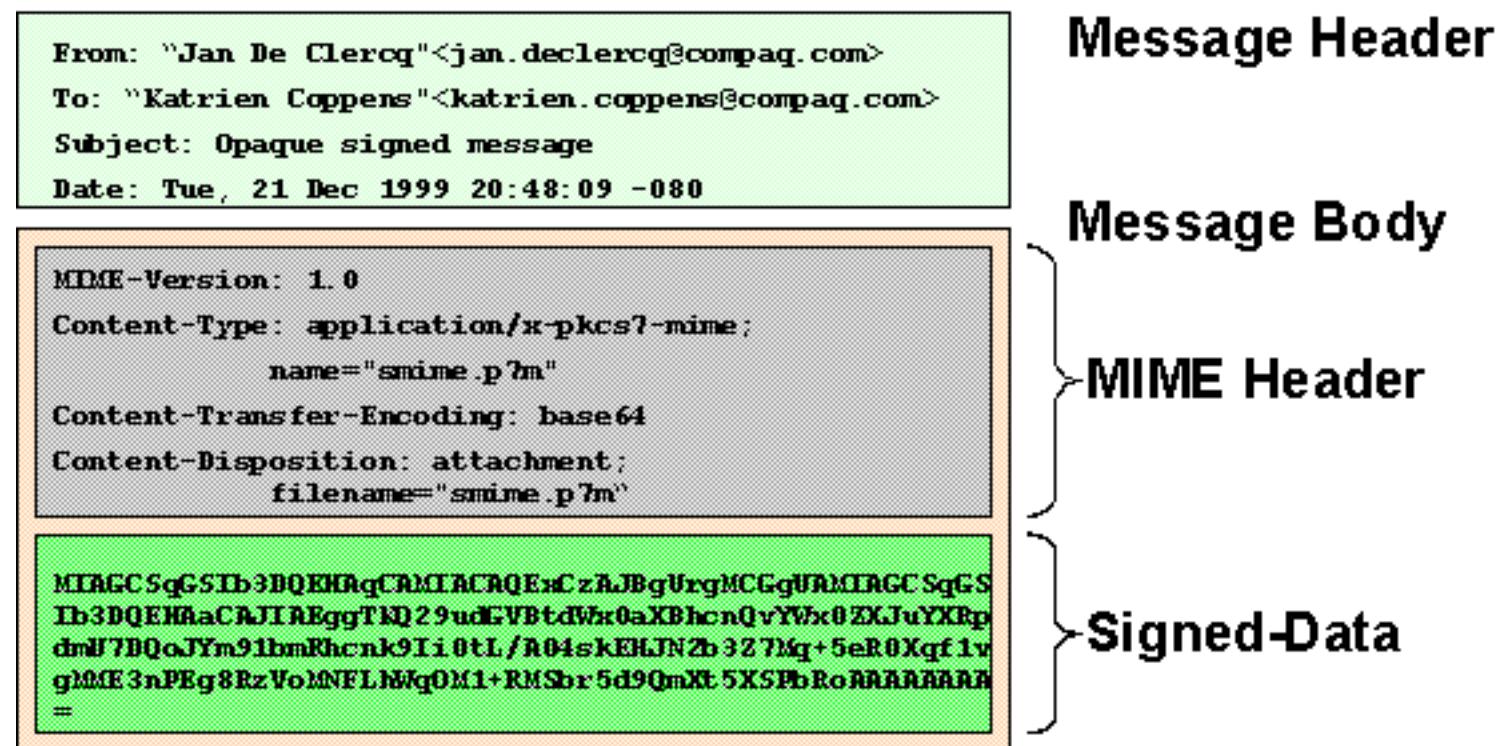
rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQ  
pfyF467GhIGfHfYT67n8HHGghyHhHUujhJh4VQpf  
yF467GhIGfHfYGTrfvbnjT6jH7756tbB9Hf8HHGT  
rfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghy  
HhHUujpfyF4 0GhIGfHfQbnj756YT64V

# Funkcije: *signed-data*

- sadržaj bilo kojeg tipa + jedan ili više digitalnih potpisa
  - obično jedan sadržaj + jedan potpis
- digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
  - moguće i više potpisnika, paralelno
  - podaci o potpisniku (certifikat, identifikator algoritma, šifrirani sažetak) pohranjuju se u vrijednost *SignerInfo*
- sadržaj i sažetak (sažeci) kodiraju se prema base64 u vrijednost *SignedData*
- funkcija osigurava autentičnost, cjelovitost i neporecivost
- korisnik mora podržavati S/MIME za čitanje i verificiranje potpisa

# *Signed data*

## Opaque Signed Message



<http://windowsitpro.com/exchange-server/advanced-security-exchange-2000-part-2>

# Potpisana poruke: application/pkcs7-mime

Content-Type: application/pkcs7-mime;  
smime-type=signed-data;  
name=smime.p7m

Content-Transfer-Encoding: base64

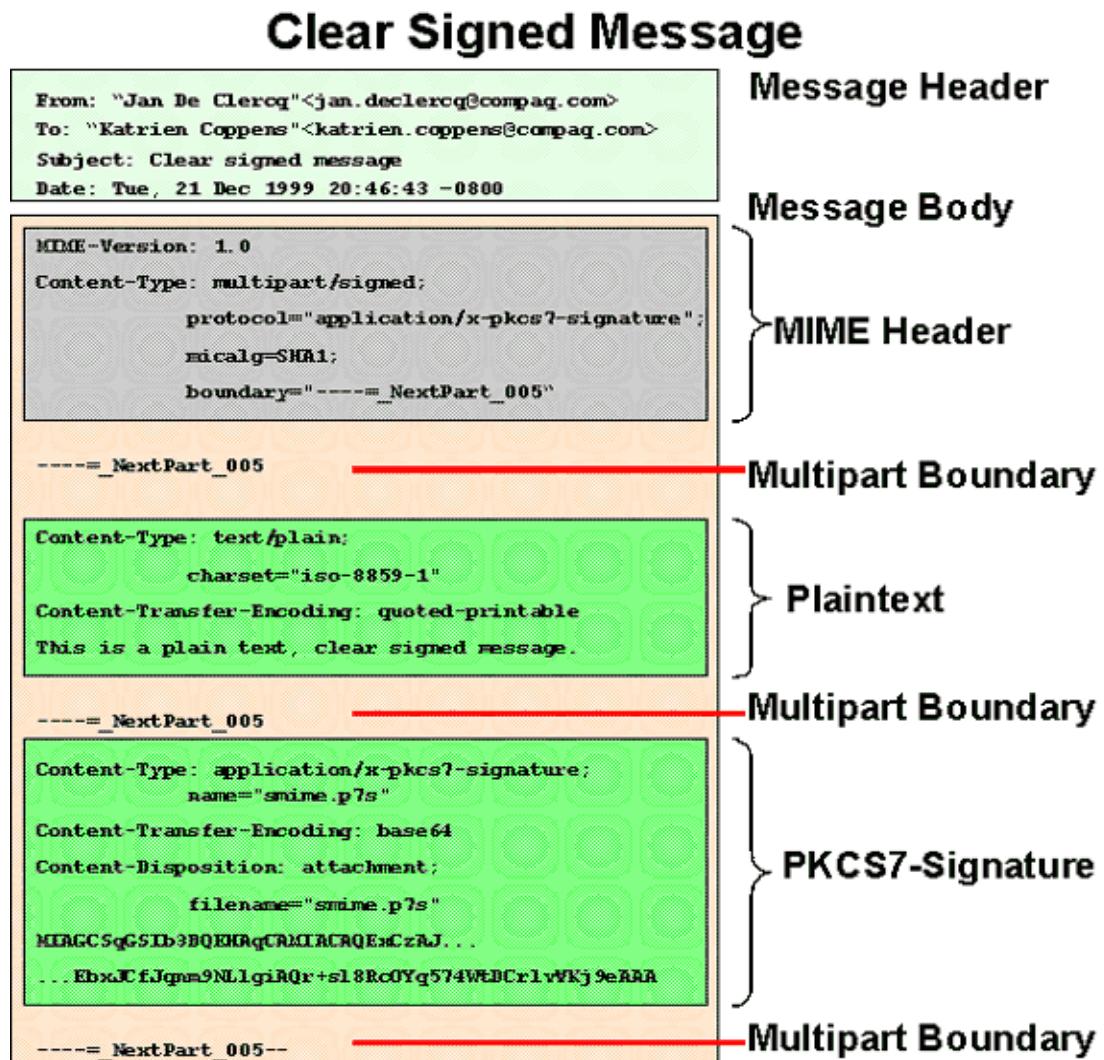
Content-Disposition: attachment;  
filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhj  
H776tbB9HG4VQbnj777n8HHGT9HG4VQpfyF467Gh  
IGfHfYT6rfvbnj756tbBghyHhHUujhJhjHHUujhJ  
h4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H  
7n8HHGghyHh6YT64V0GhIGfHfQbnj75

# Funkcije: *clear-signed-data*

- digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
  - moguće i više potpisnika, paralelno
  - podaci o potpisniku pohranjuju se u vrijednost *SignerInfo*
  - *SignedData* je prazan
- samo se sažetak (sažeci) kodira prema base64
  - sadržaj se kodira ako je neprikladan za prijenos, ali posebno
- korisnik koji ne podržava S/MIME može čitati, ali ne može verificirati potpis

# *Clear - signed data*



# Primjer potpisane poruke

```
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
```

```
--boundary42
```

```
Content-Type: text/plain
```

Ovo je potpisana poruka s tekstom u čitljivom obliku.

```
--boundary42
```

```
Content-Type: application/pkcs7-signature; name=smime.p7s
```

```
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment; filename=smime.p7s
```

```
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT64VQpfyF467Gh
IGfHfYT6jh77n8HHGghyHhHUujhJh756tbB9HGTrfvbnjn8HHGTrfvhJhjH776tbB9HG4
VQbnj7567GhIGfHfYT6ghyHhHUujpfyF47GhIGfHfYT64VQbnj756
```

```
--boundary42--
```



# Kriptografski algoritmi kod S/MIME-a

- MUST/SHOULD
- hash: preporuka SHA-1, obavezno podržavati MD5
- digitalni potpisi: DSS i RSA
- šifriranje privremenih ključeva: ElGamal i RSA
- šifriranje poruka: 3DES, RC2/40 i ostale
- definiran postupak koji određuje koji se algoritmi koriste

# Formiranje poruka prema standardu S/MIME

- poruke su kombinacija tijela prema standardu MIME i tipova podataka prema CMS-u
  - jedan format za enveloped-only
  - nekoliko formata za signed-only
  - nekoliko formata za signed i enveloped

# Certifikati

- korisnici moraju nabaviti certifikate prije upotrebe
- sukladno standardu X.509, v3
  - hibrid hijerarhije X.509 i PGP-a (web of trust)
- praksa:
  - različiti parovi ključeva za potpisivanje i šifriranje
  - moguće šifirati bez da korisnik ima svoj certifikat (par ključeva)
    - klijenti koji podržavaju S/MIME traže da korisnik instalira svoj certifikat prije nego što šifrira poštu drugima
- osnovni osobni certifikat (class 1) dokazuje da je pošta došla s adrese navedene u polju From:, no ne dokazuje identitet korisnika
- certifikat od CA (class 2) – identificira i verificira korisnika
- postoje i više klase

# S/MIME u praksi

- svi klijenti ne upravljaju dobro poštom (attachment smime.p7s)
- problemi s čitanjem pošte preko weba (webmail)
- S/MIME šifrira s kraja na kraj
  - ako je u pošti malware, on će proći neprimijećen - rješenja?
- traži certificiranje
  - nije svima prihvatljivo ili praktično
- nije moguće indeksiranje šifrirane elektroničke pošte
- mogući napadi:
  - prijava pod tuđim imenom, class 1
  - korišenje jednog certifikata, potpisivanje drugog korisnika
  - krivotvorenje zaglavlja poruke



Povjerljivost komunikacije

OpenPGP

# Pretty Good Privacy

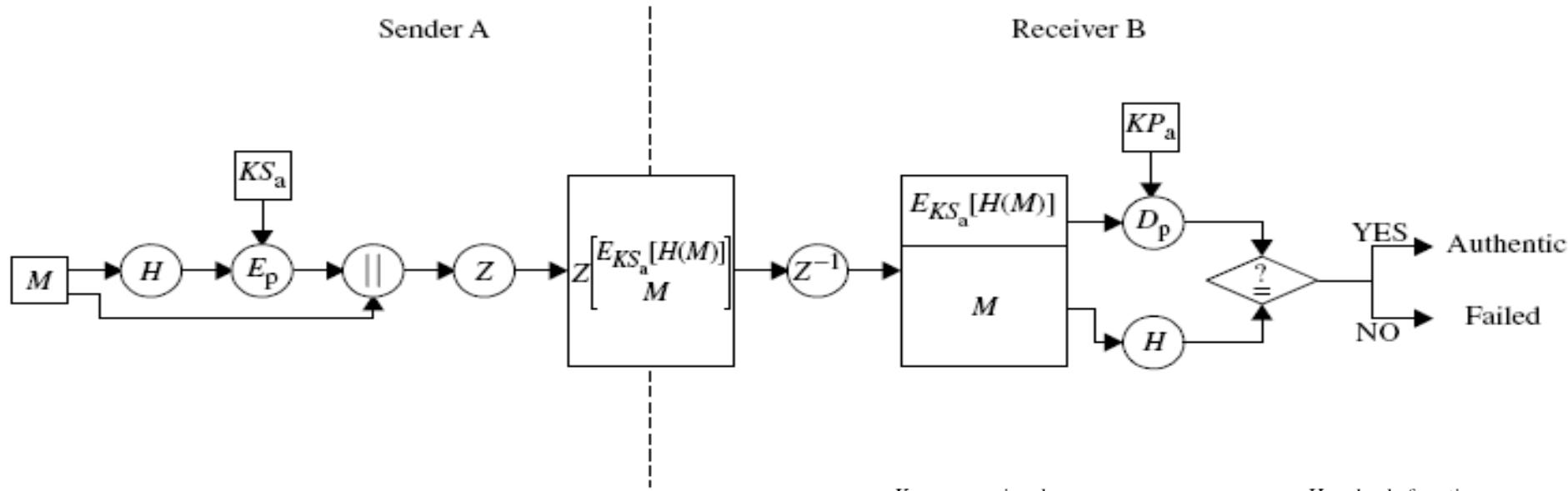
- PGP ima svoju opsežnu povijest
  - Free Software Foundation: GnuPG (GPG)
- trenutačno RFC 4880
- dostupan kao plugin u mnogim alatima



# Usluge PGP-a

- pet osnovnih usluga
  - autentifikacija (potpis/verifikacija)
  - povjerljivost (šifriranje/dešifriranje)
  - sažimanje (kompresija)
    - dobro i za šifriranje!
  - kompatibilnost s infrastrukturom elektroničke pošte
  - segmentacija i ponovno slaganje poruke
- posebno: upravljanje ključevima
- posljednje tri korisnicima su transparentne

# Digitalni potpis

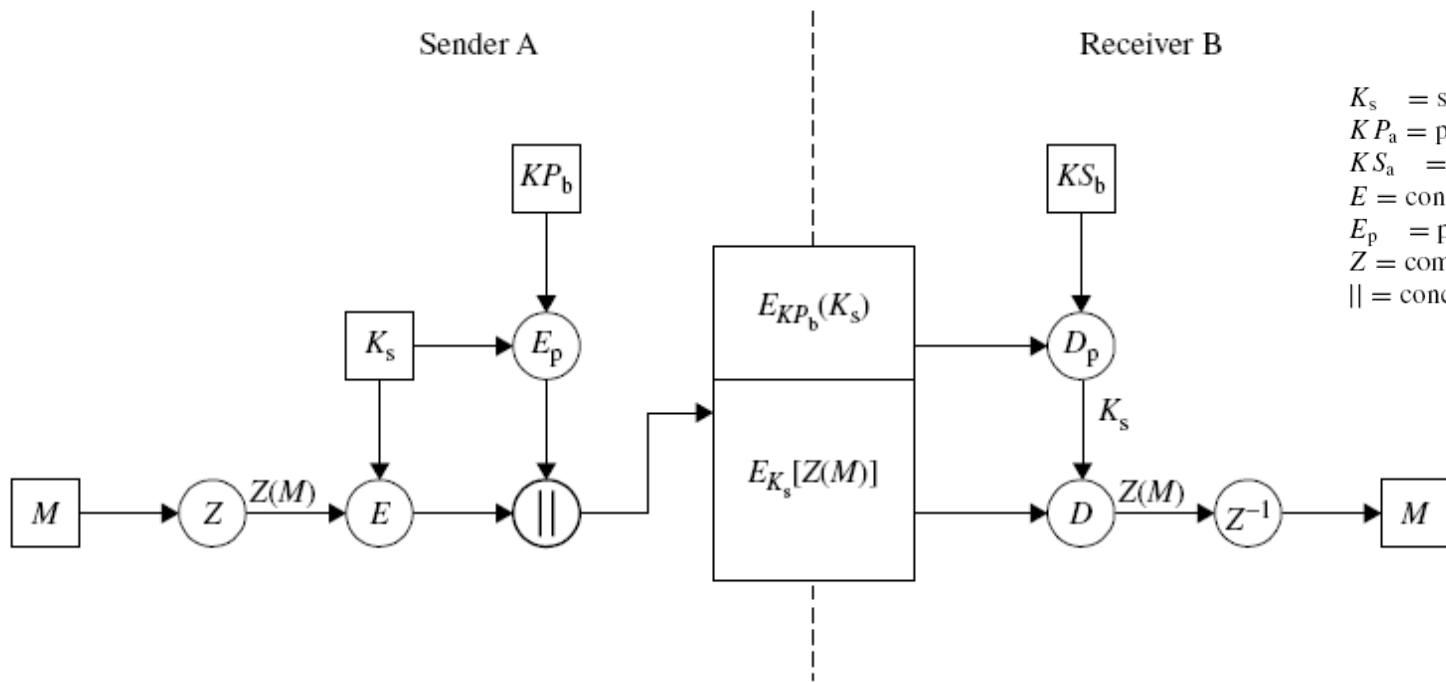


$KS_a$  = session key  
 $KP_a$  = public key of user A  
 $KS_b$  = private key of user A  
 $E$  = conventional encryption  
 $E_p$  = public-key encryption  
 $Z$  = compression using zip algorithm  
|| = concatenation

$H$  = hash function  
 $KP_b$  = public key of user B  
 $KS_b$  = private key of user B  
 $D$  = conventional decryption  
 $D_p$  = public-key decryption  
 $Z^{-1}$  = decompression

# Šifriranje

- primatelj ne može znati identitet pošiljatelja (nema autentifikacije)!
- pošiljatelj zna da samo primatelj može čitati poruku

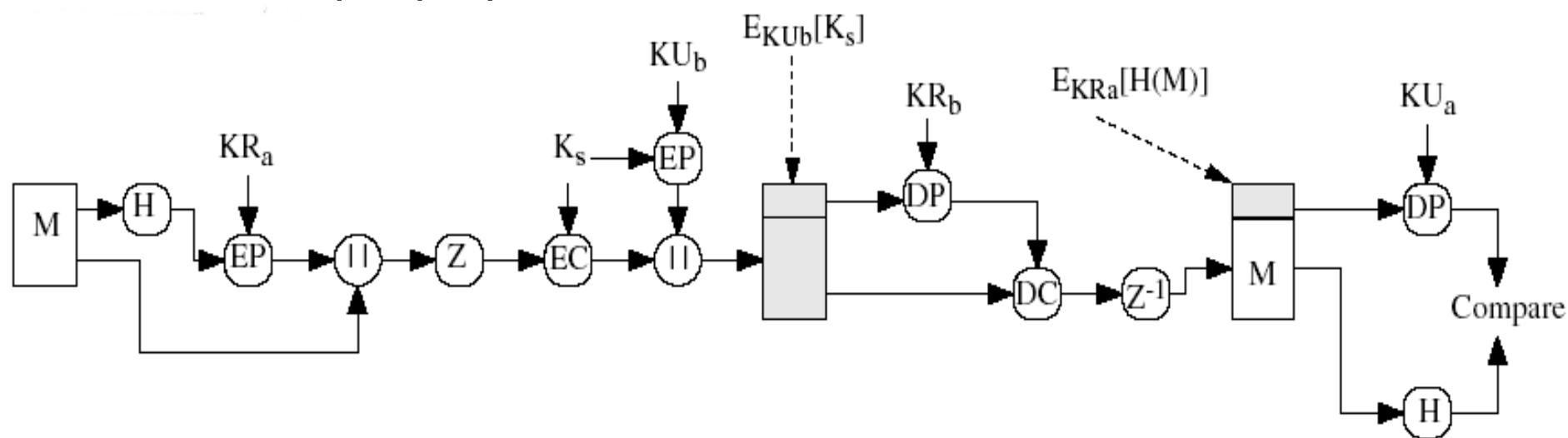


$K_s$  = session key  
 $KP_a$  = public key of user A  
 $KS_a$  = private key of user A  
 $E$  = conventional encryption  
 $E_p$  = public-key encryption  
 $Z$  = compression using zip algorithm  
 $\parallel$  = concatenation

$H$  = hash function  
 $KP_b$  = public key of user B  
 $KS_b$  = private key of user B  
 $D$  = conventional decryption  
 $D_p$  = public-key decryption  
 $Z^{-1}$  = decompression

# Šifriranje i digitalni potpis

- poruka se može potpisati i šifrirati
  - autentificirana povjerljivost



# Sažimanje

- sažimanje se događa nakon digitalnog potpisa
  - lakše kasnije verificirati ako se pohrani poruka
  - moglo bi se dinamički sažimati prije verifikacije, ali
    - sve implementacije bi morale koristiti isti algoritam sažimanja
    - ali, različite implementacije koriste različite algoritme
- obavlja se prije šifriranja
  - sažimanje smanjuje redundantnost i otežava kriptoanalizu
  - manje korištenje prijenosnih resursa
  - korisno kad se napadi temelje na frekvenciji pojave slova
- podržan: ZIP

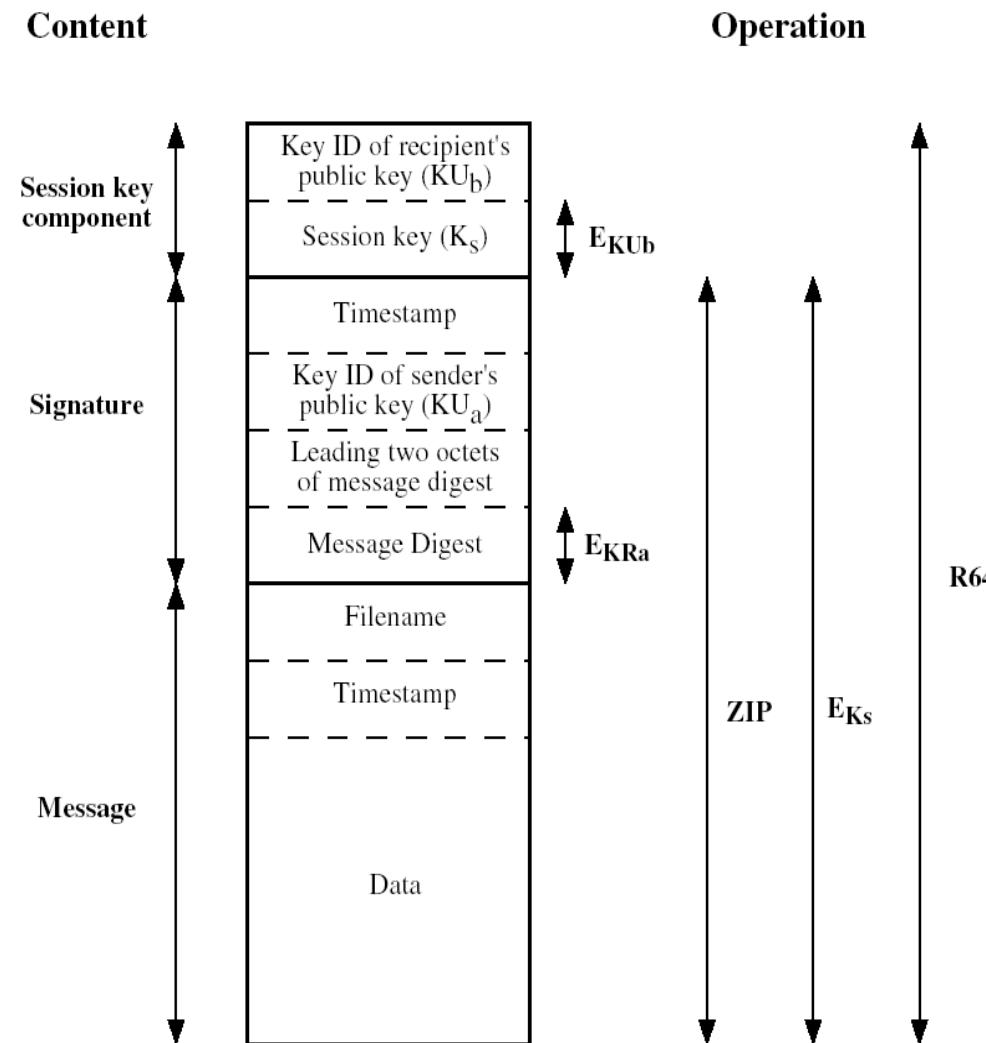
# Kompatibilnost

- kompatibilnost s infrastrukturom
- nema nikakve doticaje s privicima
  - jednako radi i u jednostavnim i u složenim sustavima
    - dakako, mora postojati plugin/alat koji zna šifrirati i dešifrirati
  - šifrirani i sažeti sadržaj pretvara se u niz ASCII znakova
    - Radix-64 / base64
    - posljedica: datoteke veće 33%

# Algoritmi

- digitalni potpis
  - DSS/SHA ili RSA/SHA
- šifriranje
  - AES, 3DES, IDEA ili CAST (simetrično)
  - Diffie-Hellman ili RSA (asimetrično)
- sažimanje
  - ZIP
- kompatibilnost
  - Radix-64
- identifikacija ključa?

# Format poruke



# Ključevi

- PGP podržava više parova ključeva po svakom pošiljatelju ili primatelju
- ključevi se pohranjuju lokalno na “privjesku” - *PGP Key Ring*
  - baza podataka
- privatni ključevi čuvaju se šifrirani
  - ID ključa: zadnja 64 bita javnog ključa
- ključ za dešifriranje poruke određuje se temeljem tzv. *passphrase*
  - javni ključevi služe za šifriranje jednokratnih simetričnih ključeva i verifikaciju potpisa
  - privatni ključevi služe za dešifriranje simetričnih ključeva i potpisivanje
- odakle ključevi i kako im se može vjerovati?

# Upravljanje ključevima

- modeli povjerenja
  - izravno povjerenje
  - hijerarhija povjerenja
  - “*web of trust*”
- nema središnjeg autoriteta
- pojedinci jedni drugima “potpisuju” ključeve
  - takvi “certifikati” pohranjuju se s ključevima na “privjesku”
- PGP izračunava razinu povjerenja za svaki ključ na “privjesku”
  - ovise o broju potpisa na javnom ključu
  - razini povjerenja u svaki od “ovjeravajućih” potpisa
  - povremeno se preračunavaju
- korisnici sami interpretiraju razine povjerenja

# *Web of*

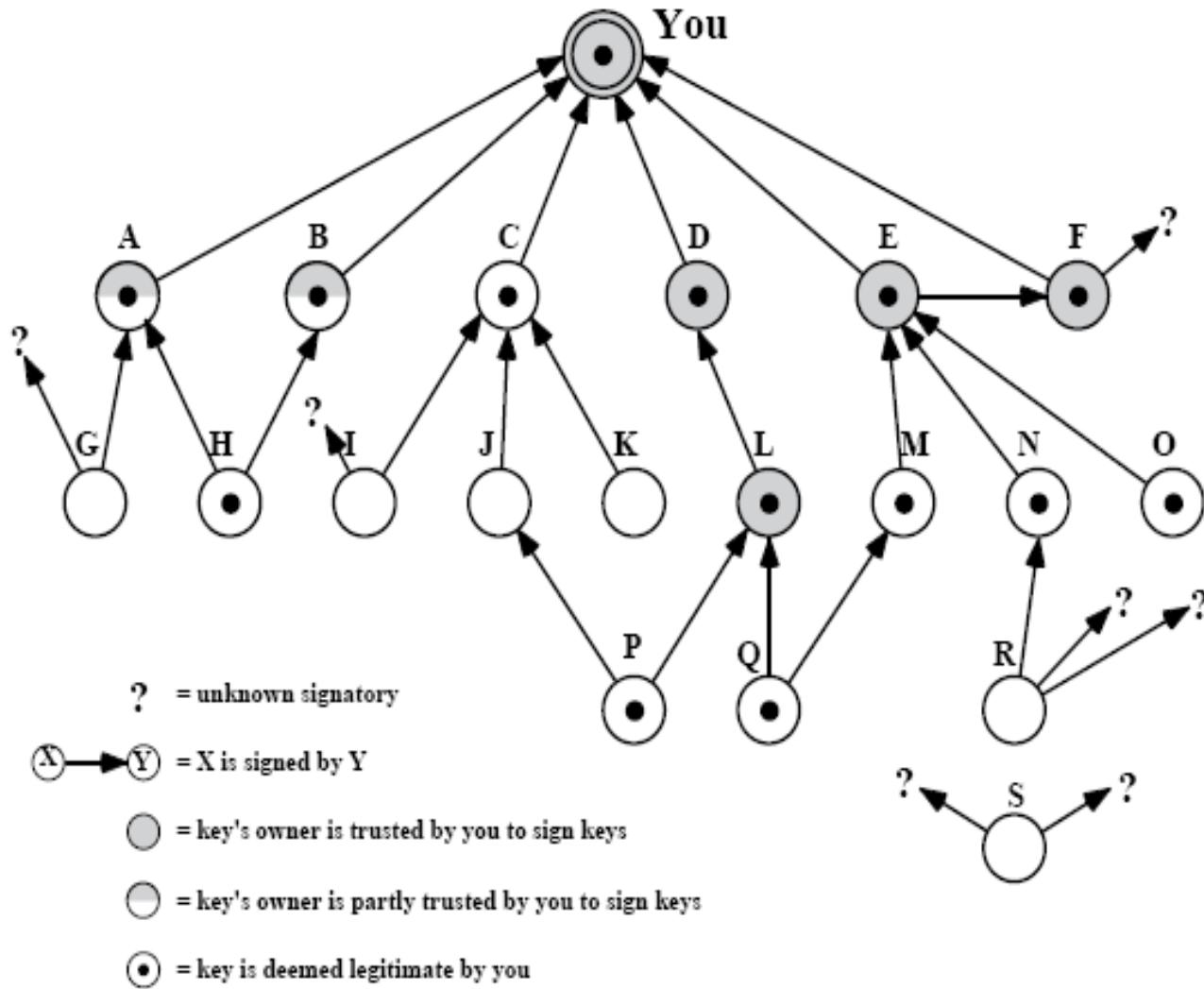


Figure 5.7 PGP Trust Model Example

# PGP i X.509

- izvorna namjera bila je da korisnici doprinose mreži povjerenja (web of trust)
  - u stvarnosti, to nije tako
- korisnici uglavnom ne razumiju o čemu se radi i ne mogu interpretirati razine sigurnosti
- kasnije verzije PGP-a podržavaju certifikate prema standardu X.509

Novije metode zaštite na razini  
poslužitelja:

**SPF, DKIM, DMARC**

# PGP i S/MIME - problemi

- PGP i S/MIME štite "s kraja na kraj"
  - Problem kod detekcije zločudnog koda / phishinga (IDS, AV) zbog šifriranja
  - Složeno za većinu korisnika?
- Novija rješenja namijenjena zaštiti elektroničke pošte između mail poslužitelja
  - dakle ne klijenata!
- SPF: *Sender Policy Framework*
- DKIM: *DomainKeys Identified Mail*
- DMARC: *Domain-based Message Authentication, Reporting, & Conformance*

# SPF: *Sender Policy Framework*

- Kako potvrditi identitet pošiljatelja?
- U DNS se dodaju IP adrese mail poslužitelja koji smiju slati elektroničku poštu u ime određene domene

```
TXT @ "v=spf1 a include:_spf.google.com ~all"
```

Components	Description
TXT	The DNS zone record type; SPF records are written as TXT records
@	In a DNS file, the "@" symbol is a placeholder used to represent "the current domain"
v=spf1	Identifies the TXT record as an SPF record, utilizing SPF Version 1
a	Authorizes the host(s) identified in the domain's A record(s) to send e-mail
include:	Authorizes mail to be sent on behalf of the domain from google.com
~all	Denotes that this list is all inclusive, and no other servers are allowed to send e-mail

<https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability>

- Primateljev mail poslužitelj provjerava DNS SPF zapise i prima poštu samo ako zapis postoji!

# DKIM: *DomainKeys Identified Mail*

- Kako potvrditi identitet pošiljatelja?
- Digitalno potpisivanje
  - Privatni ključ (mail poslužitelja – ne korisnika!) za potpisivanje FROM: polja
  - Javni ključ mail poslužitelja dostupan putem DNS zapisa
    - Primatelj (poslužitelj) verificira potpis – ispravnost FROM: polja
- Obavezno potpisivanje FROM: polja, ostalo optionalno

```
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=researchgatemail.net; h=
message-id:date:subject:from:to:mime-version:content-type
:list-unsubscribe; s=rg; bh=pmIGvLojNdgEx4i3O6QNUqgcQYM=; b=Btp6
00wjik2ucc7Fbtq7FJtO/5gb18Y6pgj6jFuXiaGluHsguXM3FTHOXwJ5CeQJh17S
En1A5TqmW7xPzFn49h1Co7bawsYpv3rSh58vc+VCEFkGIHqu7yaWacTzStkbN3xX
7QaAuiUvBGwe4QjRArfIf2RctH/EimleSmNWan8=
```

# DMARC: *Domain-based Message Authentication, Reporting, & Conformance*

- Odgovara na pitanje: što raditi s porukom koja ne prolazi SPF/DKIM?
- Opcije
  - *none* – ignoriraj poruku
  - *quarantine* – šalje npr. u spam folder
  - *reject* – javlja pošiljatelju (mail poslužitelju) da ne prolazi provjeru
- Koristi SPF ili DKIM za autentifikaciju/verifikaciju pošiljatelja
- Dobar za analizu i reporting!
  - Tko šalje mail u moje ime?
  - Otkrivanje phishing kampanja

# Primjer...

**Authentication-Results:** **spf=pass** (sender IP is 209.15.249.184)  
smtp.mailfrom=bounce.researchgate.net; fer.hr; **dkim=pass** (signature was  
verified) header.d=researchgatemail.net;fer.hr; **dmarc=pass** action=none  
header.from=researchgatemail.net;compauth=pass reason=100

**Received-SPF:** Pass (protection.outlook.com: domain of bounce.researchgate.net  
designates 209.15.249.184 as permitted sender)  
receiver=protection.outlook.com; client-ip=209.15.249.184;  
helo=mr93.researchgate.net;

Received: from mr93.researchgate.net (209.15.249.184) by  
HE1EUR02FT024.mail.protection.outlook.com (10.152.10.181) with Microsoft SMTP  
Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id  
15.20.2495.18 via Frontend Transport; Wed, 4 Dec 2019 07:59:20 +0000

Received: from mr93.researchgate.net (localhost [127.0.0.1])  
by mr93.researchgate.net (Postfix) with ESMTP id C63363CB9  
for <marin.vukovic@fer.hr>; Wed, 4 Dec 2019 07:59:18 +0000 (UTC)

**DKIM-Signature:** v=1; a=rsa-sha1; c=relaxed; d=researchgatemail.net; h=  
message-id:date:subject:from:to:mime-version:content-type  
:list-unsubscribe; s=rg; bh=pmIGvLojNdgEx4i3O6QNUqgcQYM=; b=Btp6  
0Owjik2ucc7Fbtq7FJtO/5gb18Y6pgj6jFuXiaGluHsguXM3FTHOXwJ5CeQJh17S  
EnlA5TqmW7xPzFn49h1Co7bawsYpv3rSh58vc+vCEFkGIHqu7yaWactzStkbN3xX  
7QaAuiUvBGwe4QjRARfIf2RctH/EimleSmNWan8=

**DomainKey-Signature:** a=rsa-sha1; c=nofws; d=researchgatemail.net; h=  
message-id:date:subject:from:to:mime-version:content-type  
:list-unsubscribe; q=dns; s=rg; b=E3dmXocXyHBcXUTJOMQOg8F8tRtvIC  
BxObu9oKXWo1f7Nka8FvM0arkG1vUDUXqc+Qk47jaqcAN/dx6904m1aHEkh/QsNd  
R1y+Hh7A2WX1GsOYdPfe1lfkn63YqNuresaQ7/XgZXdcjfVmp3CAZCpM9YdwXN7b  
8VazfMQtd9BHA=

<https://www.socketlabs.com/blog/the-complete-guide-to-email-authentication-part-6/>

# Primjer...

<https://www.learndmarc.com>

# Top 10 e-mail prevara

1. obitelj *Nigerian scam* prevara
2. odobreni krediti na karticama – naplaćuje se “samo” učlanjenje
3. dobitak na lotu
4. *phishing*
5. javljanje na oglas i ponuda veće cijene
6. provizija na bankovne transakcije (slično *Nigerian scamu*)
7. dobrotvorni prilozi
8. *last minute* ponude sa skrivenim troškovima
9. ulančana pisma za zaradu novaca
10. “iznajmljivanje” računala *spammerima*

[http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams\\_10.htm](http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams_10.htm)

# Primjeri iz Hrvatske...

- *phishing* – porezna uprava

Molimo navedite sljedeće informacije točno.

**Ime:**

**Prezime:**

Molimo unesite kreditne kartice primiti povrat Vašeg novca

**Broj kartice:**

**Datum isteka:** - Mjesec - / - Godina -

**Kartice PIN:**

Ovaj iznos će biti vracen na Vašoj kartici

**Iznos:** 857.88 HRK

**Podnijeti**

Iz sigurnosnih razloga, preporucujemo vam da zatvorite preglednik nakon što ste završili postupak povrata.

# Primjeri iz Hrvatske...

-----Original Message-----

From: PRAVO\_IME <Aaron256Smith@yahoo.jp>  
Subject: Your password is PRAVI\_PW  
Date: 3 Oct 2018 05:31:01 CEST  
To: PRAVI\_PW <PRAVI\_PRIMATELJ>  
Reply-To: PRAVO\_IME <Aaron256Smith@yahoo.jp>

I do know PRAVI\_PW is your passphrase. Lets get right to point. You may not know me and you're most likely wondering why you are getting this e mail? Not a single person has compensated me to investigate about you.

Let me tell you, I actually setup a software on the adult video clips (pornographic material) website and do you know what, you visited this website to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a Remote control Desktop with a keylogger which provided me access to your display screen and also web camera. Right after that, my software collected every one of your contacts from your Messenger, FB, as well as email account. And then I made a double-screen video. First part shows the video you were watching (you have a good taste omg), and second part displays the view of your cam, and it is u.

You have only 2 options. Lets look at these types of possibilities in aspects:

First option is to neglect this email message. In this case, I am going to send out your video to just about all of your contacts and then think about about the disgrace you can get. Furthermore in case you are in a loving relationship, just how it can affect?

Number 2 alternative will be to pay me \$1000. Let us name it as a donation. In this case, I will quickly eliminate your video recording. You will carry on your life like this never took place and you will never hear back again from me.

You'll make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1NuZv1BedveeZr4nwZXh7cwaTwSemkJYMG  
[CASE-sensitive, copy & paste it]

If you have been looking at going to the law enforcement, well, this email message cannot be traced back to me. I have covered my moves. I am also not looking to ask you for very much, I would like to be rewarded.

You have one day to make the payment. I've a unique pixel within this message, and at this moment I know that you have read this e-mail. If I do not receive the BitCoins, I will definately send out your video recording to all of your contacts including friends and family, coworkers, and many others. Nonetheless, if I do get paid, I'll erase the video immediately. If you need proof, reply with Yea! then I will send your video recording to your 12 friends. This is a nonnegotiable offer and so please don't waste mine time & yours by replying to this message.

-----Original Message-----

# Literatura

- svi navedeni RFC-ovi
- [www.tcpipguide.com](http://www.tcpipguide.com)
- [www.gnupg.com](http://www.gnupg.com)
- [www.openpgp.com](http://www.openpgp.com)



SVEUČILIŠTE U ZAGREBU



Fakultet  
elektrotehnike i  
računarstva

Diplomski studij

Ak. godina 2022/2023

# Sigurnost komunikacija

Sigurnost u mobilnoj telefoniji



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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/>.

# Kako je sve počelo...

- 1970-te:
  - prve pokretne mreže (“1G”)
  - analogno, ograničeno
  - FDMA
- 1980-te:
  - evolucija mreža
  - prijedlog GSM-a
- 1990-te:
  - prva komercijalna GSM mreža u Finskoj
  - druga generacija mreža (2G)
    - TDMA, CDMA
  - 1997. mobilni Internet
    - WAP (Wireless Application Protocol)

# Kako je sve počelo - sigurnost... (1/2)

- fizička sigurnost
  - uvijek aktualan problem
  - gubitak uređaja
  - količina informacija na uređaju nekada i danas nije ista!
- razina signala
  - prislушкиvanje
    - bežično ili fizički na baznoj stanici
  - ometanje
    - emitiranje na istoj frekvenciji
  - 1986. - Electronic Communication Privacy Act

# Kako je sve počelo - sigurnost... (2/2)

- identifikacija korisnika
  - SIM kartica (Subscriber Identity Module) – tajni ključ
  - šifriranje komunikacije - algoritam A5
  - kod UMTS-a – USIM – duži ključ
- identifikacija uređaja
  - tijekom prijave na mrežu
  - IMEI (International Mobile Equipment Identity)
- mobilni Internet
  - WTLS (WAP Transport Layer Security)
    - dosta problema, 3 klase (šifriranje i certifikati)
    - WAP Gap - “rupa” tijekom prijelaza s WTLS-a na SSL/TLS

# Sigurnost u mobilnoj telefoniji

- tradicionalno
  - fizička razina
    - gubitak uređaja
  - razina radio signala
    - ometanje signala, prisluškivanje
  - signalizacija
    - identifikacija korisnika i uređaja
- “pametni” telefoni
  - sigurnost aplikacija
  - *bluetooth*
  - *malware*
  - *RFID sniffing*
  - uskraćivanje usluge (DoS)
  - web aplikacije

# Prijetnje na pametnim telefonima (1/4)

- sigurnost aplikacija
- *bluetooth*
  - *blue jacking, blue snarfing, blue bugging, blue sniping*
- *malware*
- *RFID sniffing*
- uskraćivanje usluge (DoS)
- web aplikacije

# Prijetnje na pametnim telefonima (2/4)

- gubitak privatnosti
  - netko čita poruke, mailove, gleda slike
  - ali i: krađe podatke o kontaktima (tel. brojevi, elektronička pošta)
- financijski gubici
  - slanje SMS poruka na premium brojeve
  - krađa podataka kartica (kao web)
- krađa identiteta
  - RFID na mobitelima
  - postojeće aplikacije na uređaju često i identificiraju korisnika radi lakšeg korištenja (m-token, Facebook, Skype)

# Prijetnje na pametnim telefonima (3/4)

- pokretni uređaj sa zlonamjernom aplikacijom predstavlja prijetnju vlasniku ali i mreži na koju se spaja
- poslovna okolina (npr.)
  - mreža je dobro zaštićena prema Internetu, ali često se previđaju prijetnje "iznutra"
  - vlasnik pokretnog uređaja ne mora biti zlonamjeran niti svjestan prijetnji na vlastitom uređaju
  - ako mreža nije dobro zaštićena, virusi, crvi i trojanci mogu se neometano širiti u naizgled zaštićenoj mreži
  - potrebno dobro zaštiti bežične pristupne točke (WLAN AP)
    - firewall, detekcija napada, DMZ....

# Prijetnje na pametnim telefonima (4/4)

- pametni telefoni danas se koriste gotovo isto kao i računala
  - pregledavanje weba, plaćanje računa, elektronička pošta, trenutačno poručivanje, društvene mreže
- stoga su i rizici vezani uz aplikacije i komunikaciju gotovo isti kao i kod računala ali:
  - na telefonima je lakše doći do novca preko operatora (npr. premium SMS), uz "standardne" prevare kreditnim karticama
  - pristup lokaciji korisnika
  - percepcija telefona nije ista kao i percepcija laptopa ili stolnog računala
    - prevare se "ne očekuju" jer korisnici nisu na njih navikli
    - lakši pristup privatnim mrežama (WLAN) - napadi iznutra

# Sigurnost aplikacija - *OWASP top 10 mobile 2014*

M1: Weak Server Side Controls

M6: Broken Cryptography

M2: Insecure Data Storage

M7: Client Side Injection

M3: Insufficient Transport Layer Protection

M8: Security Decisions Via Untrusted Inputs

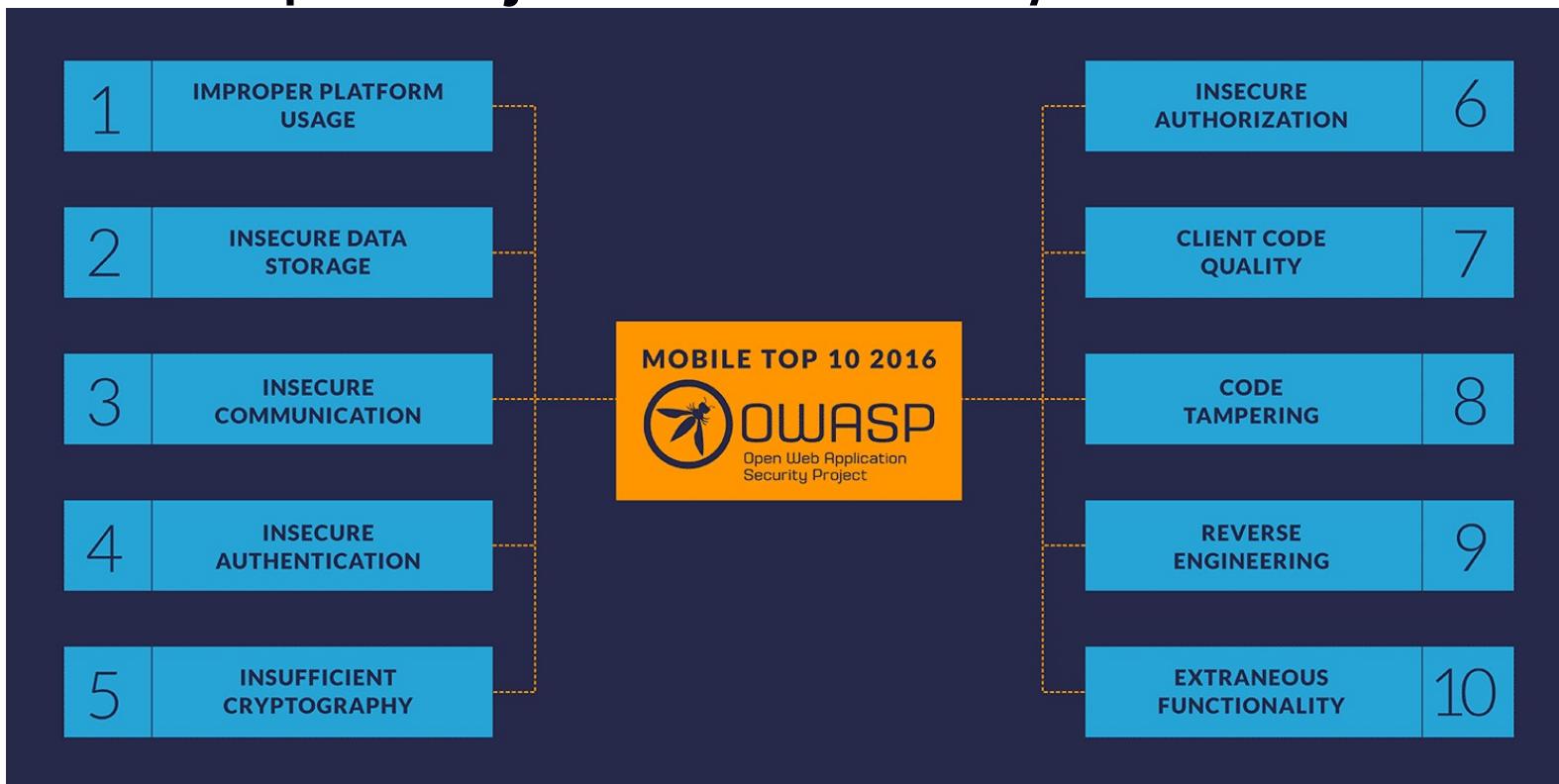
M5: Poor Authorization and Authentication

M9: Improper Session Handling

M1: Weak Server Side Controls

M10: Lack of Binary Protections

# Sigurnost aplikacija - OWASP top 10 mobile 2016



<https://www.nowsecure.com/blog/2016/10/13/secure-mobile-development-testing-owasp-mobile-top-10/>

\* Najavljenja je objava top 10 mobilnih ranjivosti za 2023

# Weak Server Side Controls

- Loša kontrola na poslužitelju
  - Obuhvaća sve što može poći po zlu na poslužitelju!
- Neki razlozi...
  - Kratki rokovi, mali budžet za sigurnost kod mobilnih aplikacija, oslanjanje na mobilni dio i zanemarivanje poslužiteljskog djela...
- Najčešći uzroci – OWASP top 10 web i OWASP top 10 cloud
  - Loša programska logika
    - ne pazi se na sve moguće obrasce korištenja usluge / aplikacije
  - Slaba autentifikacija
    - Provjera prava pristupa, kakve su lozinke, kako je proces autentifikacije zaštiće, koliko je proces autentifikacije složen
  - Upravljanje sjednicama
    - Kako se korisnici identificiraju? Je li moguće “ukrasti” sjednicu?
  - Konfiguracija poslužitelja
    - Jesu li sve komponente sigurne i ažurirane? “Cure” li podaci npr. u logove?
  - Napadi umetanjem (*injection*)
    - Umetanje SQL, javascripta i naredbi

# Insecure Data Storage

- Nesigurna pohrana “osjetljivih” podataka
- Što su uopće osjetljivi podaci?
- Europska GDPR (*General Data Protection Regulation*)
  - Različite vrste podataka su deklarirane kao osjetljive
  - Česti auditi i velike kazne!
- Podaci na mobilnom telefonu
  - Jesu li šifrirani?
  - Vide li se podaci u logovima?
  - Problem s Androidom zbog (lošijeg) *sandboxing-a*
    - Šifriranje podataka na SD kartici
    - Koristiti poseban dio sa sklopoškim šifriranjem (*secure element*)?
  - Ali i s iOS-om
    - Npr. pohrana podataka za autentifikaciju korisnika u bazu podataka aplikacije bez šifriranja

# *Insufficient Transport Layer Protection*

- Nedovoljna zaštita na transportnom sloju
- Česta ranjivost kod svih internetskih aplikacija općenito
- Gdje se sve šalju podaci iz mobilne aplikacije?
  - Jesu li ti podaci “osjetljivi”?
- Imamo li šifriranje na transportnom sloju?
- Koristiti HTTPS odnosno SSL / TLS
- Danas bi ipak ovo trebalo biti manje zastupljeno – vidjet ćemo u Top 10 za 2023.

# *Unintended Data Leakage*

- “Curenje” podataka
- Tijekom razvoja sve se zapisuje u logove a na produkciji ne bi smjelo (npr. brojevi kartica)
- Mobilne aplikacije
  - Najveći problem je priručno spremanje (*caching*)
  - Provodi se kako bi se optimiziralo izvođenje aplikacija
  - Provode ga:
    - aplikacije, radni okviri za razvoj aplikacija ali i operacijski sustav
  - Što se pohranjuje?
    - podaci, slike, tipkanje i sadržaj međuspremnika (*buffer*)
    - razvijatelji ne mogu previše na to utjecati!
- Očekivani ishod: *malware* dobije pristup pohranjenim podacima druge aplikacije

# *Poor Authorization and Authentication*

- Loša autorizacija i autentifikacija
- Glavni problemi:
  - Razvijatelji poslužiteljske strane očekuju da će samo legitimni mobilni korisnici pristupati poslužitelju
    - Ali servis je otvoren za sve kao i svaki drugi web servis...
  - Razvijatelji pogrešno smatraju kako je mehanizam spajanja na poslužitelj nevidljiv korisnicima
    - Reverznim inženjerstvom moguće je doći do koda aplikacije
    - Snimanjem mrežnog prometa moguće je vidjeti poruke i pakete
  - Mobilne aplikacije često dozvoljavaju slabije lozinke (kraće!) radi bolje uporabljivosti što olakšava napad na lozinke

# *Broken Cryptography*

- Loše upravljanje kriptografijom
  - Npr. kriptografija postoji ali ključevi su lako vidljivi napadačima
- Tipični scenariji
  - Korištenje (samo) ugrađenih mehanizama šifriranja
    - iOS šifrira kod aplikacija ali ga dešifrira prije podizanja u memoriju
    - Postoje alati koji u tom trenutku na *jailbreak* uređajima mogu doći do podataka
  - Loše upravljanje ključevima
    - Napadač može pristupiti datotekama s ključevima
    - Ključevi su zapisani u kodu aplikacije (*binary*) te napadač može doći do njih
  - Izrada vlastitih mehanizama šifriranja
    - Česte greške ako se ne posveti dovoljno vremena i znanja!
  - Korištenje zastarjelih algoritama
    - Mnogi algoritmi su već probijeni ili zahtjevaju veće duljine ključeva

# *Client Side Injection*

- Umetanje na klijentskoj strani
  - Obično se radi umetanje na poslužitelju – česta ranjivost weba (kod, SQL, javascript)
- Razmisliti o tome što sve korisnik unosi i prepostaviti da neće unositi ono što očekujemo
- Što se sve može “ubaciti”?
  - Kao i kod poslužitelja, može unositi SQL (SQLLite) ali i datoteke (*File inclusion*)
    - Npr. na poslužitelj je ubačen sadržaj koji rezultira u ovom napadu kada aplikacija učita podatke
  - Ako aplikacija koristi mobilni preglednik moguće je umetati Javascript (XSS)
  - Preplavljivanje spremnika tj. metoda / funkcija – rušenje aplikacija (npr. *jailbreak!*)
    - Npr. jedna maliciozna aplikacija radi napad na drugu aplikaciju
  - Ubacivanje koda putem binarnih datoteka

# *Security Decisions Via Untrusted Inputs*

- “Sigurnosne odluke na temelju nepovjerljivih izvora”
- Mehanizam *Inter Process Communication (IPC)*
  - Mehanizam za dijeljenje podataka između aplikacija
- Jedna aplikacija šalje ulazne podatke drugoj
  - zahtjev za lokacijom
  - autorizacija
  - prikaz podataka na karti...
- Moguće je mijenjati te podatke ili ubaciti lažne zahtjeve od strane *malwarea!*
- Ovim mehanizmom ne bi trebalo slati osjetljive podatke!
- Ako aplikacija takve podatke koristi kao ulaz onda ih treba dobro provjeriti i sanitizirati

# *Improper Session Handling*

- Loše upravljanje sjednicom
  - Kao i kod poslužitelja
  - Sjednica = pristup pravima korisnika koji je "vlasnik" sjednice
  - Sjednicu kontrolira poslužitelj a kao korisnik se identificira aplikacija
    - Kolačići (cookie), tokeni s vremenskim istekom...
- Neki primjeri iz mobilnih aplikacija
  - Problemi s odjavljivanjem na poslužitelju
    - Korisnik se odjavi u mobilnoj aplikaciji ali se to stanje ne preseli na poslužitelj
  - Vremenska kontrola
    - Često je vremenska kontrola loše izvedena ili je nema pa jedna sjednica traje predužno što otvara prostor za napadače kojima ukradena sjednica "dulje vrijedi"
    - Djelomičan razlog su i dulja trajanja sjednica na mobitelima zbog uporabljivosti aplikacija
  - Upravljanje kolačićima (rotacija)
    - Kada se korisnik prijavi trebao bi mu se izdati novi kolačić
  - Nesigurni tokeni
    - Korištenje zastarjelih tj. probijenih algoritama za kreiranje tokena

# *Lack of Binary Protections*

- Nedostatak zaštite binarnog koda aplikacije
- Glavni problem: iz binarnog zapisa moguće je doći do izvornog koda aplikacije
  - *Reverse engineering*, mnoštvo alata, npr. APKTool, ClutchMod
- U originalnu aplikaciju se nakon otkrivanja izvornog koda ubacuje dodatni kod koji se prikriva kao korisna originalna aplikacija
  - Tipičan scenarij malwarea na Androidu!
- Zaštita?
  - Detektirati je li uređaj na kojem se aplikacija izvodi “jailbreakan” ili “rootan”
  - Provjeravati zaštitnu sumu kako bi se utvrdila promjena aplikacije
  - *Certificate Pinning Controls*
    - Korištenje predefiniranih certifikata pri spajanju na vanjske usluge
    - [https://www.owasp.org/index.php/Certificate\\_and\\_Public\\_Key\\_Pinning](https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning)
  - Detektirati je li aplikacija pokrenuta u *debug* načinu rada

# *Code tampering*

- Jednom kada je aplikacija instalirana na uređaj sav kod i podaci se nalaze na uređaju
- Je li uređaj “rootan” / “jailbreakan”?
  - Root ovlast!
- Mijenjanje podataka koje aplikacija koristi
- Mijenjanje knjižnica koje aplikacija koristi
- “Put prema” reverznom inžinjeringu...

# *Reverse Engineering*

- Koliko je teško doći do izvornog koda aplikacije?
  - Obfusacija?
- Otkrivanjem izvornog koda mogu se otkriti
  - Sigurnosni mehanizmi
  - Korištenje ranjivih algoritama
  - Izbjeći neke provjere i kontrole
  - Pozadinski poslužitelji i komunikacija
  - Lokalno pohranjene lozinke, tokeni, ključevi...
- Promjena funkcionalnosti i ponovna objava aplikacije
  - Čest slučaj, ubacivanje malwarea!

# Bluetooth ranjivosti (1/3)

- većina Bluetooth (BT) platformi ima ranjivosti
  - loše implementiran BT složaj
    - ne prati se duljina paketa
    - Buffer overflow napadi
  - pogrešne IRMC (*Integrated Remote Management Controller*) dozvole na datoteke
    - otvorene konekcije omogućuju pristup svim uređajima, a ne samo uparenim
  - loše implementirane usluge temeljene na BT
    - česti propusti u implementaciji koji omogućuju neovlaštene upade i pregledavanje datoteka na uređaju
  - otvoreni kanali
    - korisnici nisu svjesni prijetnji pa uređaj ostaje vidljiv i nakon korištenja (npr. nakon BT slušalica u vozilu)

# Bluetooth ranjivosti (2/3)

- *blue jacking*
  - slanje poruka na uređaj putem BT
  - najčešće reklame ovisne o lokaciji (domet 10m)
  - bezopasno, ali oblik spama
- *blue snarfing*
  - neovlašteni pristup uređaju s BT
  - pronalazi otvorene BT kanale i tim putem pristupa uređaju
  - omogućuje:
    - pregledavanje i preuzimanje kontakata, slika, kalendarja i poruka ovisno o uređaju
  - onemogućeno na novijim platformama (za sada)

# Bluetooth ranjivosti (3/3)

- *blue bugging*
  - kao bluesnarfing – napadač ostvaruje pristup uređaju žrtve
  - omogućuje slanje AT naredbi ciljanom uređaju
    - pozivanje brojeva, slanje SMS poruka
    - preusmjeravanje dolaznih poziva na uređaj napadača (uređaj se predstavlja kao BT slušalica)
- *blue sniping*
  - uobičajene BT antene dometa do 15 m (telefoni) ili do 100 m (laptop)
    - ograničenje kod napada
  - proširenje bluetooth napada većim dometom antene
    - na kućište se stavlja procesor i usmjerena antena velikog dometa koja omogućuje “snajpersko ciljanje” uređaja
    - domet do 2 km

# Malware

- virusi, trojanci i crvi
  - prvi mobilni malware identificiran 2004. godine (Mosquito)
    - trojanac skriven u igru
    - slanje SMS poruka na premium brojeve
- slični rizici kao na računalima uz “novosti”:
  - pristup lokaciji
  - pristup pokretnoj mreži (naplata)
- prijenos malwarea:
  - elektronička pošta (privitak)
  - linkovi na zlonamjerne stranice
  - instalacija naizgled korisnih aplikacija od strane korisnika
  - bluetooth
  - neizravno: nadogradnja operacijskog sustava (npr. jailbreaking)

# Malware - prijetnje

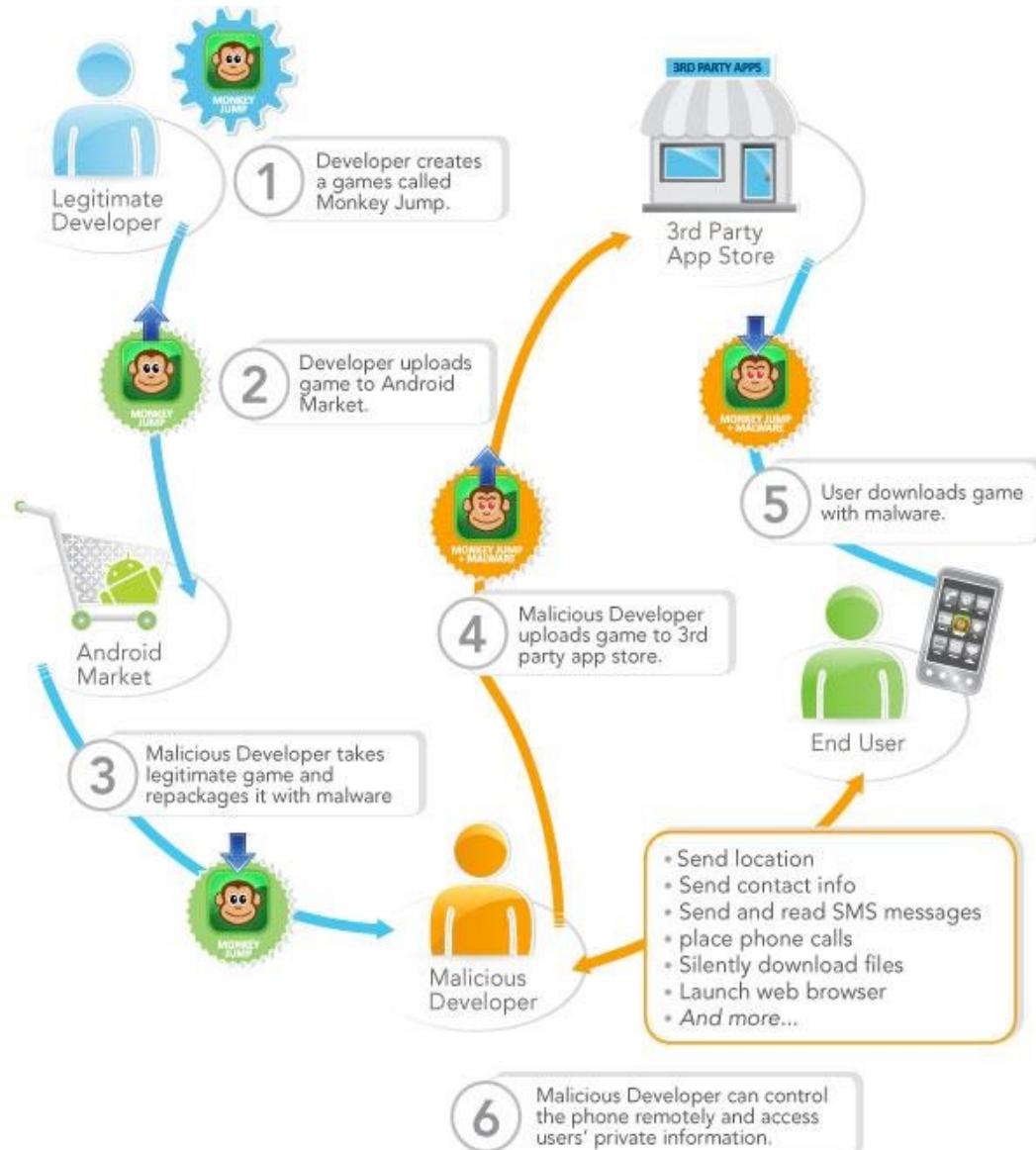
- što malware na pokretnom telefonu radi?
  - krađa lozinki
  - phishing aplikacije
    - prva 2010. na Androidu
    - predstavljala se kao aplikacija banke
  - krađa povjerljivih podataka
    - posebno lokacije korisnika
  - brisanje podataka s uređaja
  - slanje SMS poruka na premium brojeve
    - Mosquito 2004. (Symbian)
  - korištenje uređaja kao dio botneta
    - Symbian 2009.
  - uništavanje uređaja (*bricking*)

# Malware – potpisivanje aplikacija

- malware u aplikacijama - kako ga spriječiti?
  - Ideja je testirati aplikacije kako bi se utvrdilo jesu li štetne za korisnike ili treću stranu (na bilo koji način)
  - ako su aplikacije u redu onda se izdaje potpis kojim se jamči da je aplikacija prikladna (npr. code signing)
  - primjeri:
    - Java ME
      - aplikacija koja nije bila potpisana morala je uvijek pitati korisnika može li pristupiti resursima uređaja (SMS, poziv i slično)
      - jedino potpisane aplikacije su mogle pristupati resursima bez pitanja
    - iPhone
      - koncept AppStorea - Jailbreak?
    - Android
      - Android market
      - instalacija aplikacija od strane korisnika

# Tipičan scenarij

[http://appleinsider.com/articles/11/08/03/lookout\\_retrevio\\_warn\\_of\\_growing\\_android\\_malware\\_epidemic\\_note\\_apps\\_ios\\_is\\_far\\_safer](http://appleinsider.com/articles/11/08/03/lookout_retrevio_warn_of_growing_android_malware_epidemic_note_apps_ios_is_far_safer)



# Malware – operacijski sustavi - Android

- Android
  - najugroženiji zbog velikog broja korisnika
  - trend malwarea
    - lipanj 2010. – siječanj 2011 – porast 400%!
    - Q1 2012 – porast od 1200%
    - 2012. – porast od 2180%!
  - preko 80 aplikacija je uklonjeno s Android Marketa jer su sadržavale maliciozan kod
  - glavna prijetnja
    - “provaljene” igre koje se inače naplaćuju
  - Danas često: *adware* (primjer kasnije)

# Malware – operacijski sustavi - iOS

- iOS
  - prilično siguran zahvaljujući kontroli AppStorea i općenito (pre)restriktivnoj politici Applea
  - ipak, aplikacije koje korisničke profile pohranjuju na webu mogu biti predmet napada
  - Apple zapisuje kretanje korisnika? – baš i ne!
  - problem: *jailbreak*
    - omogućuje korisnicima da preuzimaju aplikacije iz drugih izvora
      - veliki rizik malwarea
    - većina korisnika nakon jailbreaka ostavlja početnu root lozinku
  - 2014. - *Keylogger* kao posljedica grešaka u implementaciji sustava
  - 2016. - Pegasus

# Pegasus

- 2016.
- Iskorištavao ranjivosti Apple iOS do verzije 9.3.5.
  - *CVE-2016-4655: Information leak in Kernel – A kernel base mapping vulnerability that leaks information to the attacker allowing him to calculate the kernel's location in memory.*
  - *CVE-2016-4656: Kernel Memory corruption leads to Jailbreak – 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to secretly jailbreak the device and install surveillance software.*
  - *CVE-2016-4657: Memory Corruption in Webkit – A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.*
- Klikom na poveznicu telefon se “jailbreaka”, instalira se malware koji čita poruke, prati pozive, lokacije...

# AdWare – Android, 2019

- 2019.
- 42 aplikacije u Google Play Store-u s AdWare-om (istim)
  - Android/AdDisplay.Ashas
- Nakon instalacije legitimne aplikacije
  - adware se pokreće kao pozadinski servis
  - komunicira s C&C poslužiteljem i šalje podatke o uređaju, OS-u...
- U nasumična vremena podiže transparentni ekran preko aktivne aplikacije s oglasom
  - nasumičnost - teže za povezati iz koje aplikacije je inicijalno pokrenut
  - Zavarava korisnika korištenjem lažnih imena procesa (paket com.google.xxx)
- Kreator pronađen preko C&C poslužitelja (Vijetnam)
  - Zanimljivo: OSINT (Open Source INTelligence)
- <https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/>

# RFID sniffing (1/2)

- RFID (Radio Frequency IDentification)
  - antena pobuđuje oznaku (tag) koja koristi EM polje antene kako bi odaslala vlastiti identifikator
  - neki noviji telefoni imaju ugrađene oznake (Nokia, Samsung, HTC...)
- RFID oznaka jedinstveno identificira korisnika
  - alternativa kreditnim karticama, članskim iskaznicama, kod evidencije radnog vremena....
- problem sigurnosti
  - pretpostavimo da pokretni telefon (ugrađeni tag ) jedinstveno identificira korisnika
  - ako napadač ukrade ID korisnika može se lažno predstavljati!

# RFID sniffing (2/2)

- sigurnost je trenutačno problem kod tehnologije RFID
- zaštita
  - šifriranje podataka na oznaci
    - npr. MIFARE / DESFIRE (studentske Xice)
  - ograničeni doseg antene
    - NFC antena odašilje na nekoliko cm
    - moguće povećanje dosega (sjetimo se blue snipinga...)?
  - beskontaktno plaćanje
    - *Secure Element*
  - još se u velikoj mjeri istražuje

# Kako se štititi?

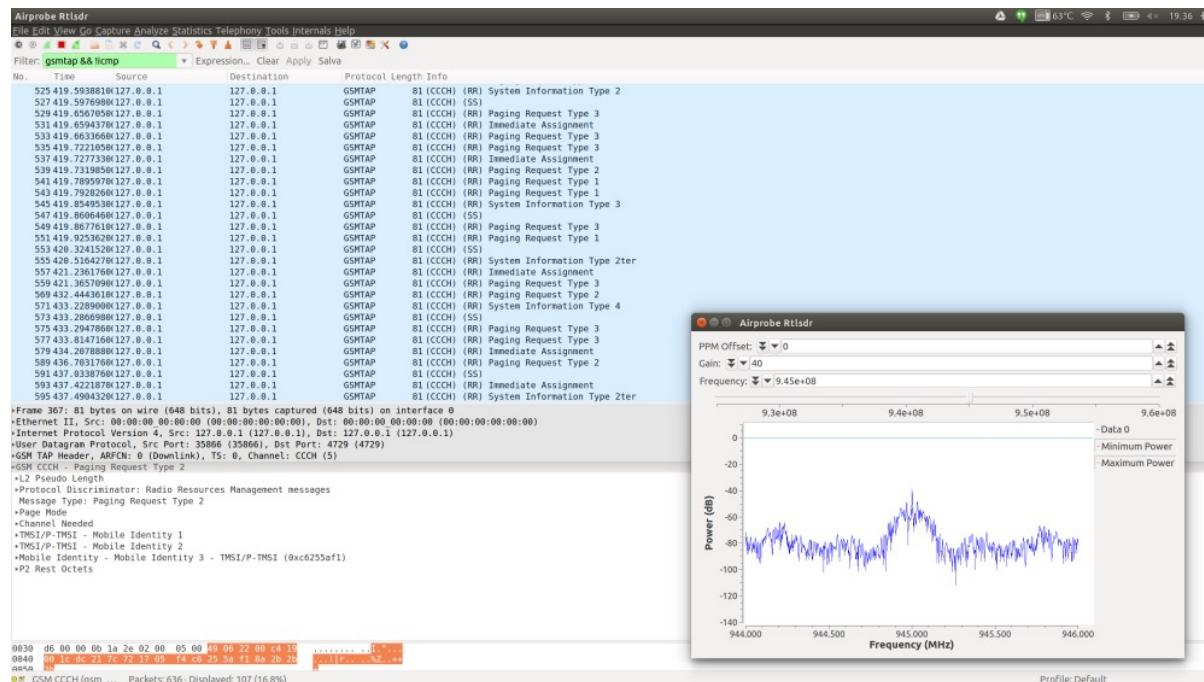
- Ažuriranje sustava na najnoviju verziju
  - posebno Android
- Ne koristiti aplikacije ili “dućane aplikacija” treće strane
- Što je s tvrtkama?
  - BYOD (*Bring Your Own Device*) politika
    - postoji već dugo za prijenosna računala, sada popularna i za pametne telefone
  - Kako osigurati da “doneseni” privatni uređaji korisnika nisu rizik za informacijsku sigurnost tvrtke?
    - Kontejnerizacija (*containerization*)

# Kontejnerizacija

- virtualna particija na pokretnom uređaju
  - na njoj se nalaze osjetljive aplikacije i podaci
  - *sandboxing* aplikacija
    - sjetimo se predavanja o operacijskim sustavima, virusima i crvima!
  - šifrirani podaci
- Uredaj ima profile
  - npr. obični i sigurni
  - nije moguće prebacivati podatke iz jednog u drugi
- Platforme
  - Apple iOS
    - standardno podržava na razini uređaja jer je tako izведен sustav
  - Android
    - potrebno instalirati dodatne platforme
    - Knox (Samsung), Divider

# Prisluškivanje mobilnog prometa?

- Uređaji SDR – *Software Defined Radio*
  - Npr. HackRF One
- Signalizacija i komunikacija – odvojeno!



# ... i što nas čeka u 2023.?

- širenje malware svih vrsta
  - ransomware
  - povećenje financijskih gubitaka
  - “malware će postati unosan posao na mobilnim platformama”
  - najviše prijetnji na Androidu
- top-lista prijetnji
  - širenje phishinga na mobilne uređaje
    - zbog sve više pametnih telefona
  - premium SMS/poziv prevare
  - botneti
    - očekuje se značajan rast aktivnih botneta
  - “rupe” u operacijskim sustavima
    - npr. *keylogger* na Apple uređajima



SVEUČILIŠTE U ZAGREBU



Fakultet  
elektrotehnike i  
računarstva

Diplomski studij

Ak. godina 2022/2023

# Sigurnost komunikacija

Sigurnost signalizacije u  
telekomunikacijskim mrežama



# Creative Commons



- **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 daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom 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/>.

# Neke ključne riječi u mobilnim mrežama

- IMSI
  - *International Mobile Subscriber Identity*
  - Određuje zemlju, operatora i jedinstveni identifikator
- MSISDN
  - *Mobile Subscriber International Integrated Services Digital Network Number*
  - Telefonski broj (npr. 385991234567)
- IMEI
  - *International Mobile Equipment Identity*
  - Jedinstveni identifikator sklopovlja / mobitela
  - Analogija s MAC adresom
- P-TMSI
  - *Packet Temporary Mobile Subscriber Identity*
  - Anonimizirani i privremeni IMSI – kako se „pravi“ IMSI ne bi slao preko signalizacijskog kanala

# Kriptografija u mobilnim mrežama

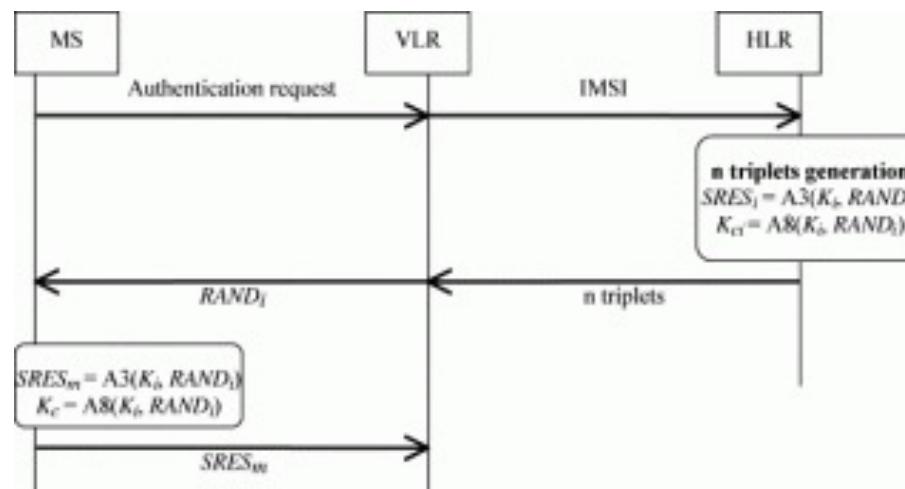
- Obitelj algoritama "A"
  - Karakterizira ih "*security by obscurity*"
  - Svaka novija generacija mreže koristi bolje algoritme
  - Stari algoritmi su probijeni!
- Jeden od načina prisluškivanja...
  - Većina operatera treba podržavati starije generacije
  - Npr. 2G ili "EDGE" u područjima slabe naseljenosti, smanjenje na 2G u uvjetima visokog prometa itd.
  - Kada dođe do nadogradnje koriste se stari algoritmi
  - Ometanje novijih mreža (npr. 5G) radi prisilnog smanjivanja razine?

# Kriptografija u mobilnim mrežama- algoritmi

- A3
  - Autentifikacijski algoritam
    - Koristi se pri spajanju na mobilnu mrežu / baznu stanicu / "toranj"
- A8
  - Algoritam za generiranje ključeva za šifriranje
  - Koristi se za generiranje sjedničkih ključeva za algoritam A5
- A5
  - Šifriranje tokova podataka (*stream*) između uređaja i baznih stanica
    - A5/0 : nema šifriranja
    - **A5/1 : LFSR šifriranje tokova, 64 bitni ključ**
    - **A5/2 : LFSR šifriranje tokova, 64 bitni ključ**
    - A5/3 : KASUMI, 128 bitni ključ
    - A5/4 : 128 bitni ključ, kao A5/3

# Autentifikacija u mobilnim mrežama - GSM

- Simetrično šifriranje
  - Simetrični ključ pohranjen u sigurnosnom elementu na SIM kartici (SE, HSM)
  - Operater također ima isti ključ (naravno)
  - Zašto se ne koristi asimetrična kriptografija?



<https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/>

# Autentifikacija u mobilnim mrežama

- Problemi s GSM-om?
  - Nema autentifikacije baznih stanica / „tornjeva”
    - „IMSI catchers” i napadi MITM
  - Loši i probijeni algoritmi
- Dobre stvari u 3G/LTE/UMTS
  - Bolji algoritmi (KASUMI)
  - Duži ključevi
  - *Authentication and Key Agreement*
    - Autentifikacija bazne stanice putem MAC-a
  - Ipak, ne zaboravimo: moguće ometanje kako bi se koristila starija tehnologija...

<https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/>

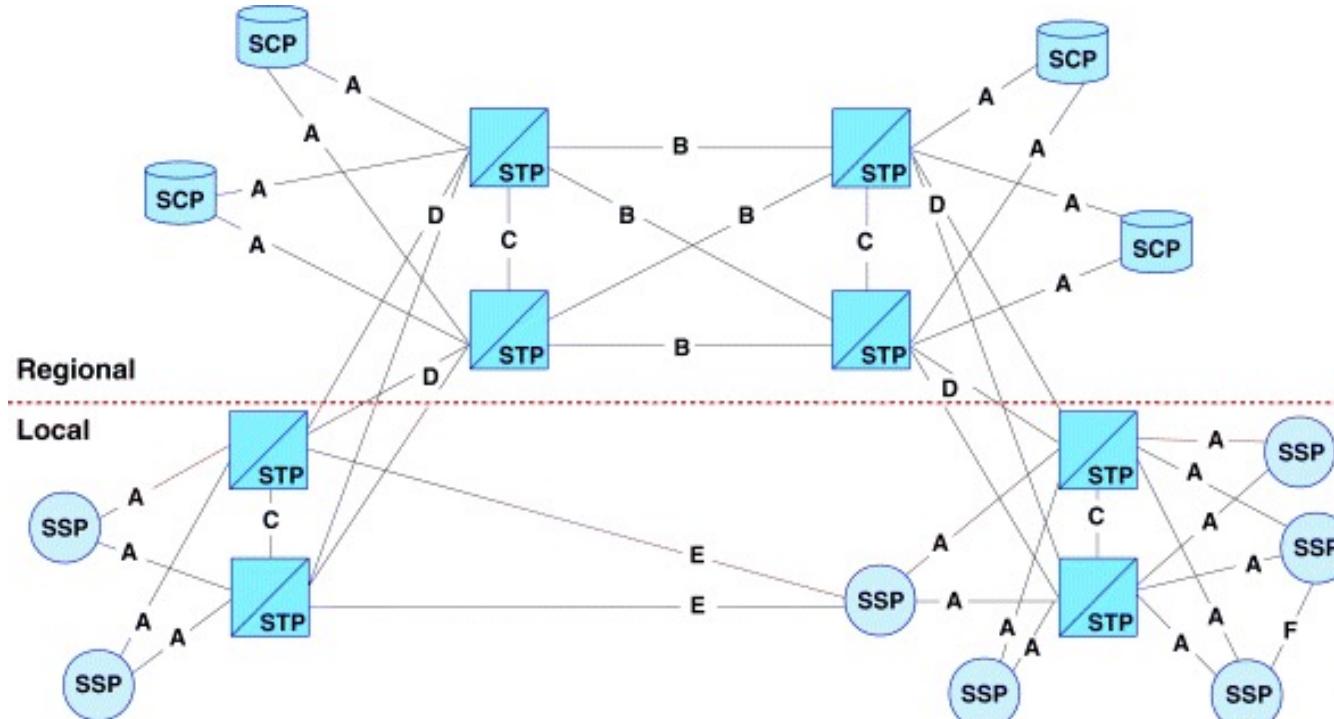
# Signalizacija u telekomunikacijskim mrežama

- Specifičnost: odvojeni kanali za signalizaciju i promet
- Danas najkorišteniji protokol - *Common Channel Signaling System no. 7* - (CC)SSNo7 ili **SS7**
  - Osmišljen tijekom 70ih, standard tijekom 80ih
  - Zadužen za kontrolu poziva – uspostavljanje i prekidanje
  - Odvojeni kanal za signalizaciju
  - SMS se prenosi preko signalizacije!
- Danas se SS7 koristi u svim telekomunikacijskim mrežama
  - I za povezivanje različitih mreža (npr. više operatora mobilne mreže)
- Temelji se na povjerenju između mreža / davaljatelja usluge
  - Autentifikacija?

# Signalizacija u telekomunikacijskim mrežama

- Sjetimo se:
  - evolucija mreža je velikim dijelom okarakterizirana uvođenjem IP složaja u jezgrenu mrežu
- „SS7 u IP mrežama” = SIGTRAN (*signaling transport*)
  - Omogućuje korištenje SS7 u mrežama temeljenim na IP-u
  - SIGTRAN koristi *Stream Control Transmission Protocol* (SCTP) za slanje signalizacije u IP mrežama
- *Stream Control Transmission Protocol*
  - Protokol transportnog sloja
  - UDP paketi

# Arhitektura SS7

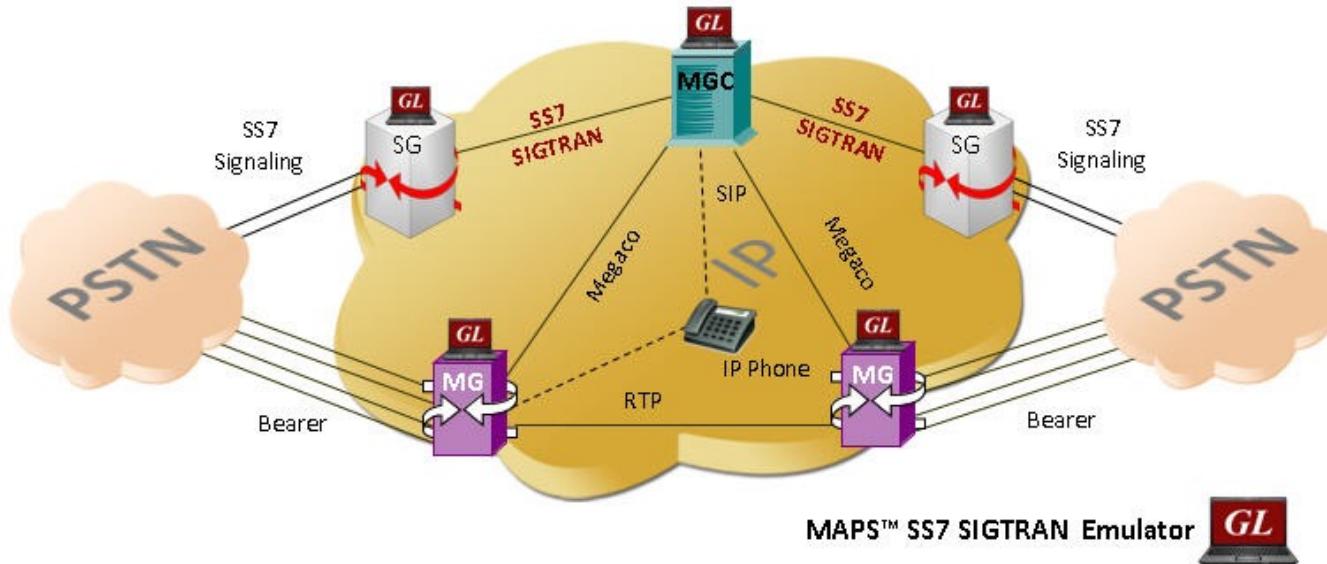


[https://docstore.mik.ua/univercd/cc/td/doc/product/tel\\_pswt/vco\\_prod/ss7\\_fund/ss7fun02.htm](https://docstore.mik.ua/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun02.htm)

SSP – Signal Switching Point

STP – Signal Transfer Point

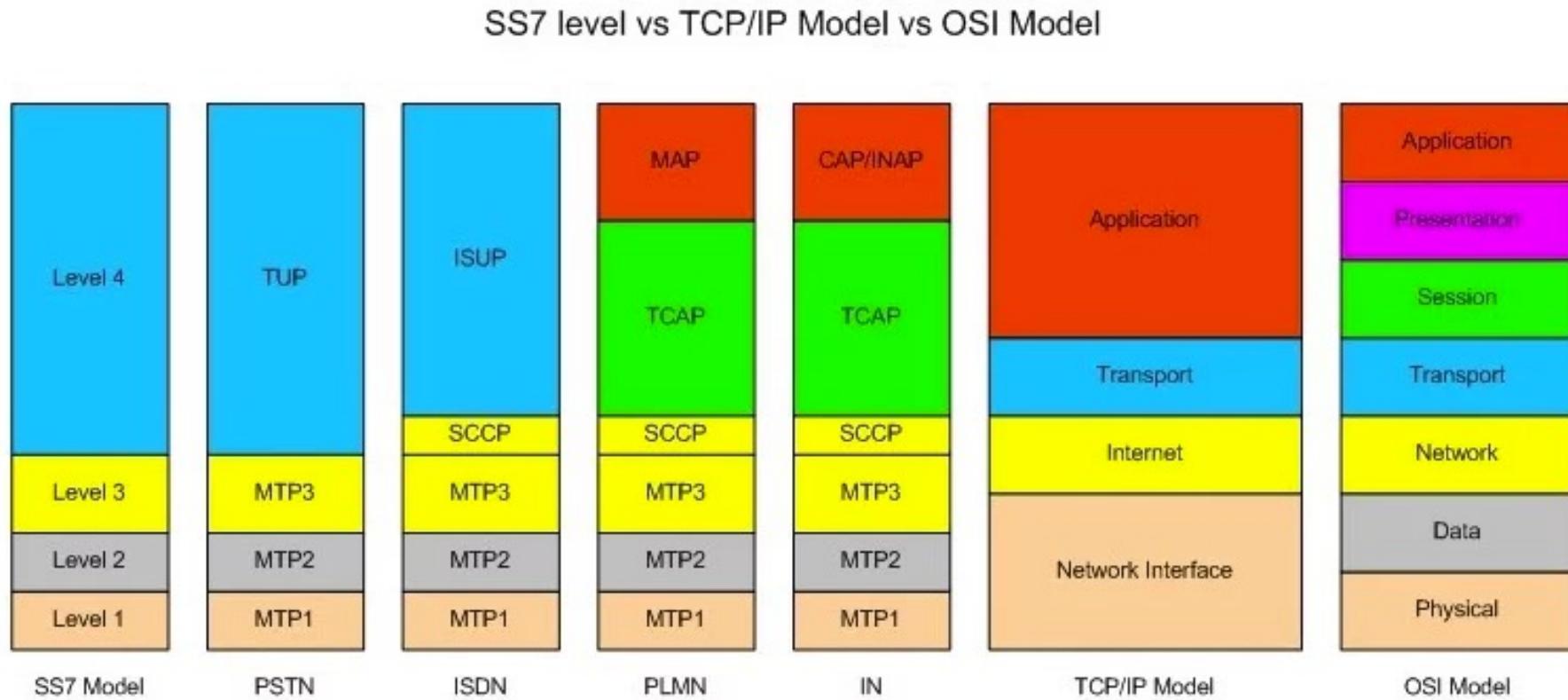
# Arhitektura SS7 u IP mrežama



<https://www.gl.com/maps-sigtran.html>

- Potencijalni problem
  - Spoj različitih mreža
    - tehnološki istih, a pogotovo različitih
  - Tipično - lokalno VoIP preko protokola SIP, u jezgri SS7

# SS7 i mapiranje na različite modele



MTP – Message Transfer Part (1 - physical, 2 - data link layer, 3 - network)

SCCP – Signalling Connection Control Part

TCAP – Transaction Capabilities Application Part

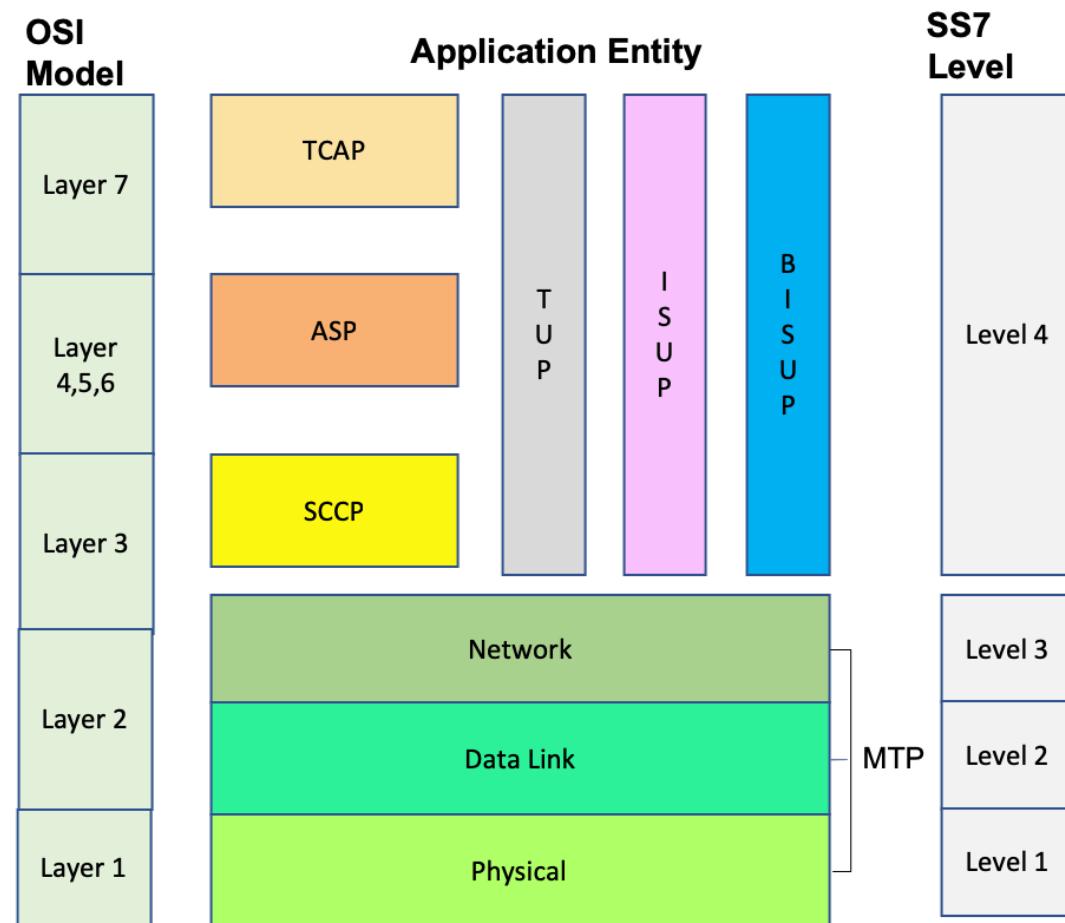
MAP – Mobile Application Part

TUP – Telephone User Part

ISUP – ISDN user Part

BISUP – Broadband ISDN User Part

# SS7 vs OSI



<https://www.firstpoint-mg.com/blog/ss7-attack-guide/>

TCAP: Transaction Capabilities Application Part  
ASP: Application Service Part  
SCCP: Signaling Connection Control Part  
TUP: Telephone User Part  
ISUP: ISDN User Part  
BISUP: Broadband ISDN User Part  
MTP: Message Transfer Part

# Napadi u SS7 – krađa IMSI

- IMSI (*International Mobile Subscriber Identity*)
  - Broj mobitela (+385...)
- Ipak – na zračnom sučelju vidi se TMSI (*Temporary IMSI*)
  - Napadač očita TMSI
- Ako napadač ima pristup SS7 može tražiti IMSI koji odgovara TMSI-ju
- Može se koristiti za povredu anonimnosti, praćenje...

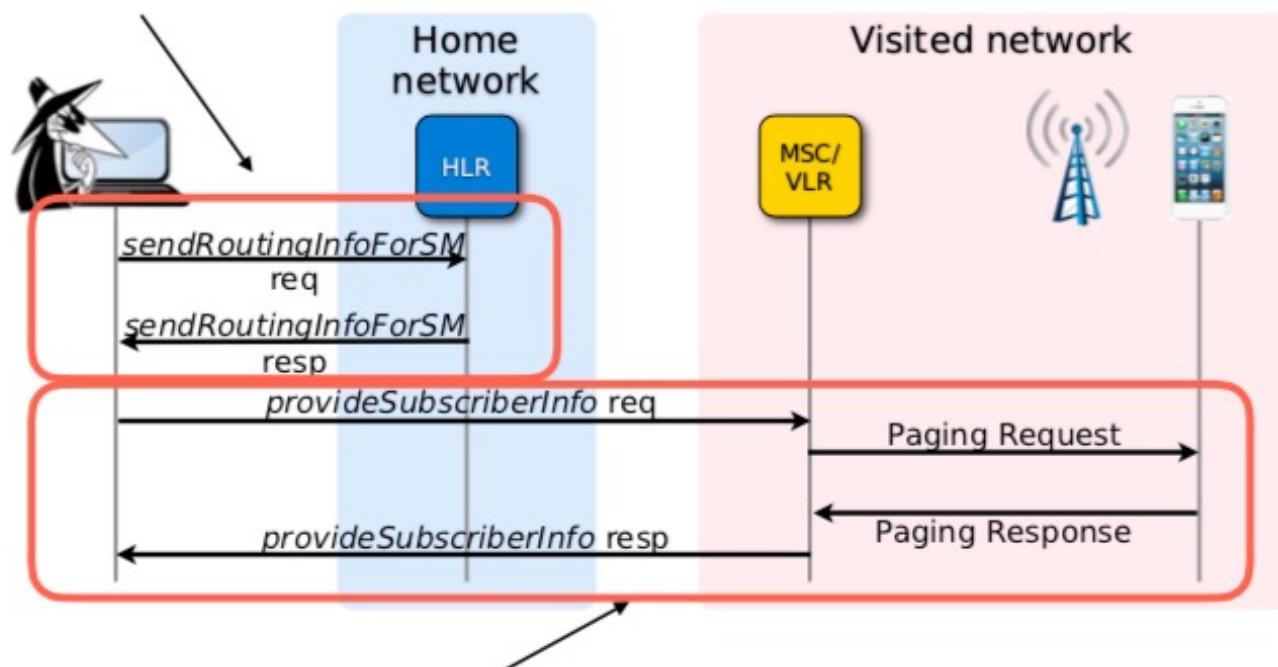
# Napadi u SS7 – otkrivanje lokacije korisnika

- Napadač se predstavlja kao „strani” HLR (VLR?) i kontaktira HLR (*Home Location Register*)
  - HLR – baza podataka o korisnicima „domaće” mreže, (VLR – *Visitor LR*)
- Šalje MAP poruke s upitom o korisniku
  - *Mobile Application Part* (MAP)
    - Protokol aplikacijskog sloja za razmjenu informacija između čvorova mobilne mreže
  - Kao odgovor dobija:
    - *Cell ID* (CID) – ćelija mobilne mreže, npr. 46033
    - *Mobile Country Code* (MCC) – kod države, npr. 219 za HR
    - *Mobile Network Code* (MNC) – kod mobilne mreže, npr. 02 je Telemach u HR
    - *Location Area Code* (LAC) – kod lokacijskog područja, npr. 1
  - <http://www.cell2gps.com/>, <https://www.radiocells.org/>

# Napadi u SS7 – praćenje lokacije korisnika

## Step 1: Get IMSI and address of current MSC

- *Send-Routing-Info-for-SM-Request (SRR)*
  - Dolazi poziv/SMS – gdje je korisnik?
- *Paging*
  - Mreža mora uvijek znati gdje je korisnik
  - Paging poruke ga “pozivaju” i traže



## Step 2: Request the cell id of the subscriber to the current MSC

[https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN\\_AS19/cellular-security.pdf](https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf)

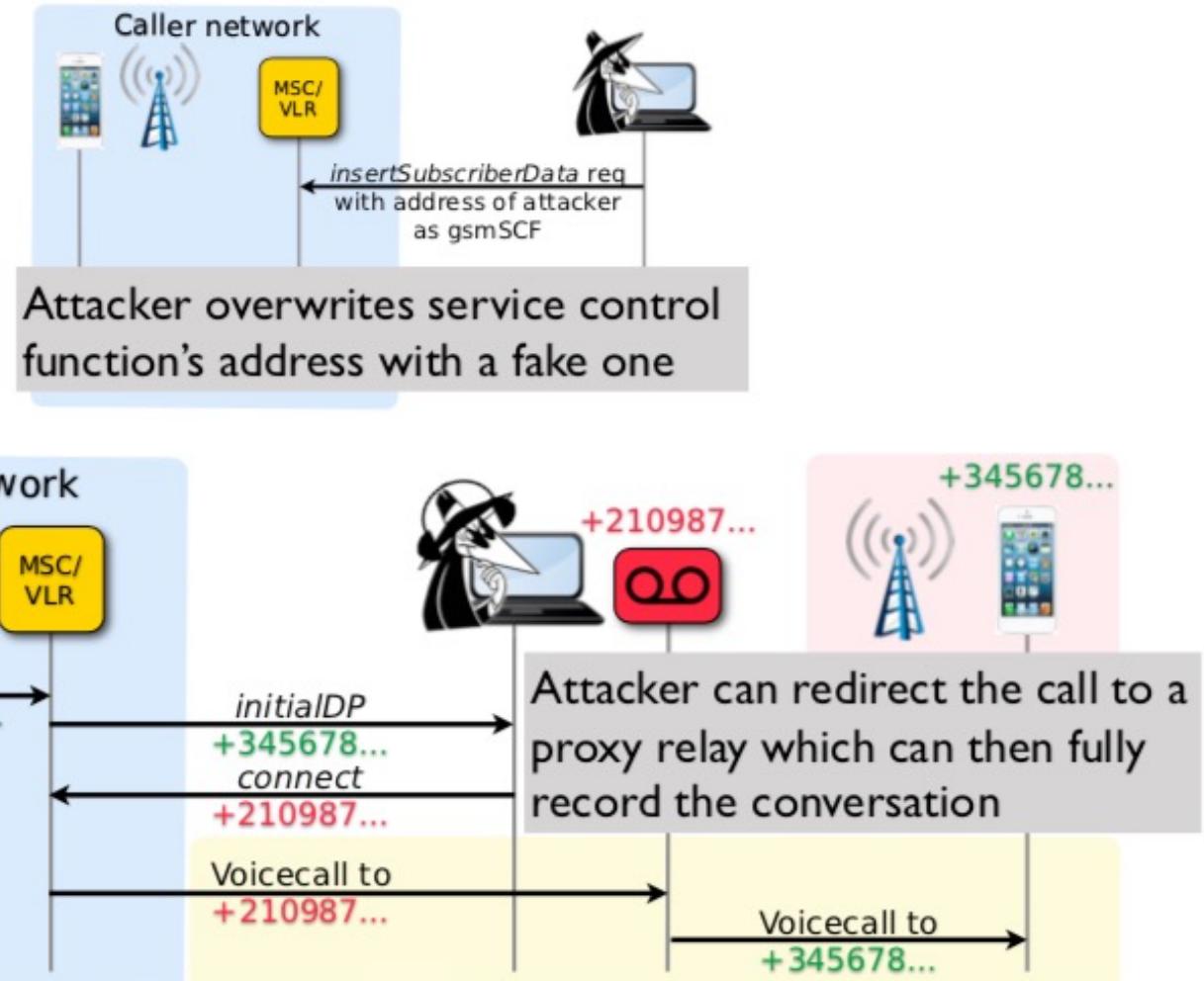
# Napadi u SS7 – prislушкиvanje

- Moguće prislушкиvanje dolaznih i odlaznih poziva bez obzira na napadačevu lokaciju u mreži u odnosu na žrtvu (domaća, roaming)
  - <https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/>
- Odlazni poziv
  - Koriste se dodatne funkcionalnosti IN (*Intelligent Network*) koje su osmišljene za razvoj usluga s dodanom vrijednosti u fiksnim mrežama (PSTN)
  - *Customized Applications for Mobile network Enhanced Logic* (CAMEL)
    - Usluge s dodanom vrijednosti koje proširuju GSM
    - Korisno za napadače – usluga nadzire pozive korisnika iz domaće mreže kada je u roaming
    - CAMEL usluge su “smještene” u gsmSCF – *GSM Service Control Functions*
  - Napadač koristi CAMEL kako bi odlazne pozive preumsjerio k sebi, a zatim ih prosljeđuje na pravo odredište - MITM

# Napadi u SS7 – prislушкиvanje

- Moguće prislушкиvanje dolaznih i odlaznih poziva bez obzira na napadačevu lokaciju u mreži u odnosu na žrtvu (domaća, roaming)
  - <https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/>
- Dolazni poziv
  - Sličan princip kao kod odlaznog poziva
  - No, jednostavniji jer se koriste uobičajene funkcije za prosljeđivanje poziva
  - Napadač putem MAP poruka proslijedi poziv k sebi a zatim uspostavlja novi poziv prema žrtvi
  - Ponovno MITM!

# Prisluškivanje



[https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN\\_AS19/cellular-security.pdf](https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf)

# Napadi u SS7 – presretanje poruka SMS

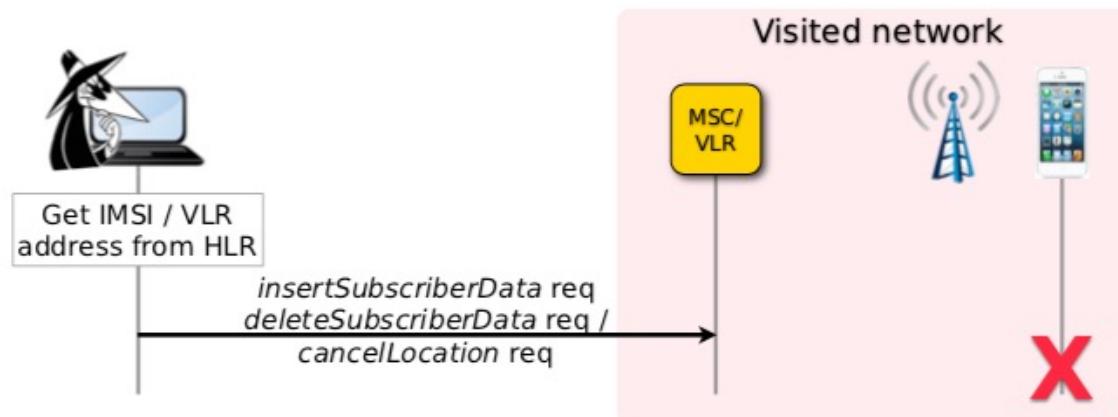
- Napadač se lažno predstavlja kao MSC ili VLR (*Mobile Switching Center* ili *Visitor Location Center*) i traži promjenu lokacije u ime žrtve
- Šalje MAP poruku *Update Location* na žrtvin HLR
  - Smisao: promijeno sam lokaciju, nova lokacija žrtve je napadač, tj. njegov lažni MSC / VLR
- Nakon toga, mreža misli da je žrtva na novoj lokaciji (ili u drugoj mreži ako je lažni VLR) i tamo šalje SMS poruke namijenjene žrtvi
- Problem: MFA, kodovi za usluge, bankarstvo...

# Napadi u SS7 – lažiranje USSD zahtjeva

- *Unstructured Supplementary Service Data (USSD)*
  - Koristi se npr. za slanje zahtjeva za nadoplatu prepaid računa
  - Ali i ozbiljnije stvari, npr. mobilna bankarstva
- Koncept je da se napadač lažno predstavlja kao žrtva i traži nadoplatu, kod ili neku transakciju
- Nakon pokretanja transakcije, presereće SMS namijenjen žrtvi tako da žrtva nije uopće svjesna da se nešto događa

# Napadi u SS7 – uskraćivanje usluge

- Očigledno se može manipulirati signalizacijom (prethodni slideovi)
  - Prema tome, uskraćivanje usluge se može izvesti na više načina!



[https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN\\_AS19/cellular-security.pdf](https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf)

# Još neki problemi

- Sve navedeno podrazumijeva da napadač ima pristup signalizacijskoj mreži i SS7
  - Očekivali bismo da je to teško izvedivo
- Ipak, SCTP čvorovi dostupni su na mreži!
  - *Well-known ports* definirani
  - SCTP – 4-way handshake
- *SCTP ranjivosti*
  - [https://nvd.nist.gov/vuln/search/results?form\\_type=Basic&results\\_type=overview&query=SCTP&search\\_type=all&isCpeNameSearch=false](https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=SCTP&search_type=all&isCpeNameSearch=false)
- SCTPscan - Finding entry points to SS7 Networks & Telecommunication Backbones
  - <https://www.p1sec.com/corp/research/tools/sctpscan/>
  - <https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf>

# Privatnost?

- CDR - Call data records
- Anonimizacija i deanonimizacija
- Analiza i predviđanje kretanja, tko priča s kim...

Caller SIM	Callee SIM	Outgoing BTS	Incoming BTS	Timestamp	Call duration (sec)
0458685984	0488595496	12	365	2018-01-18 15:22:12	456
0458685984	0458685984	12	25	2018-01-18 22:24:12	35
0469875254	0498563201	879	567	2018-01-19 08:47:10	125
(...)	(...)	(...)	(...)	(...)	(...)

[https://www.researchgate.net/figure/Sample-of-typical-call-data-records\\_tbl1\\_325681249](https://www.researchgate.net/figure/Sample-of-typical-call-data-records_tbl1_325681249)

# Literatura

- Tobias Engel: SS7: Locate. Track. Manipulate.
  - [https://www.youtube.com/watch?v=-wu\\_pO5Z7Pk](https://www.youtube.com/watch?v=-wu_pO5Z7Pk)
- 8 SS7 vulnerabilities you need to know about
  - <https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/>
- Signalling Security in Telecom SS7/Diameter/5G - ENISA
  - <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g>
- SCTPscan - Finding entry points to SS7 Networks & Telecommunication Backbones
  - <https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf>