SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

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 daljnjeg 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.

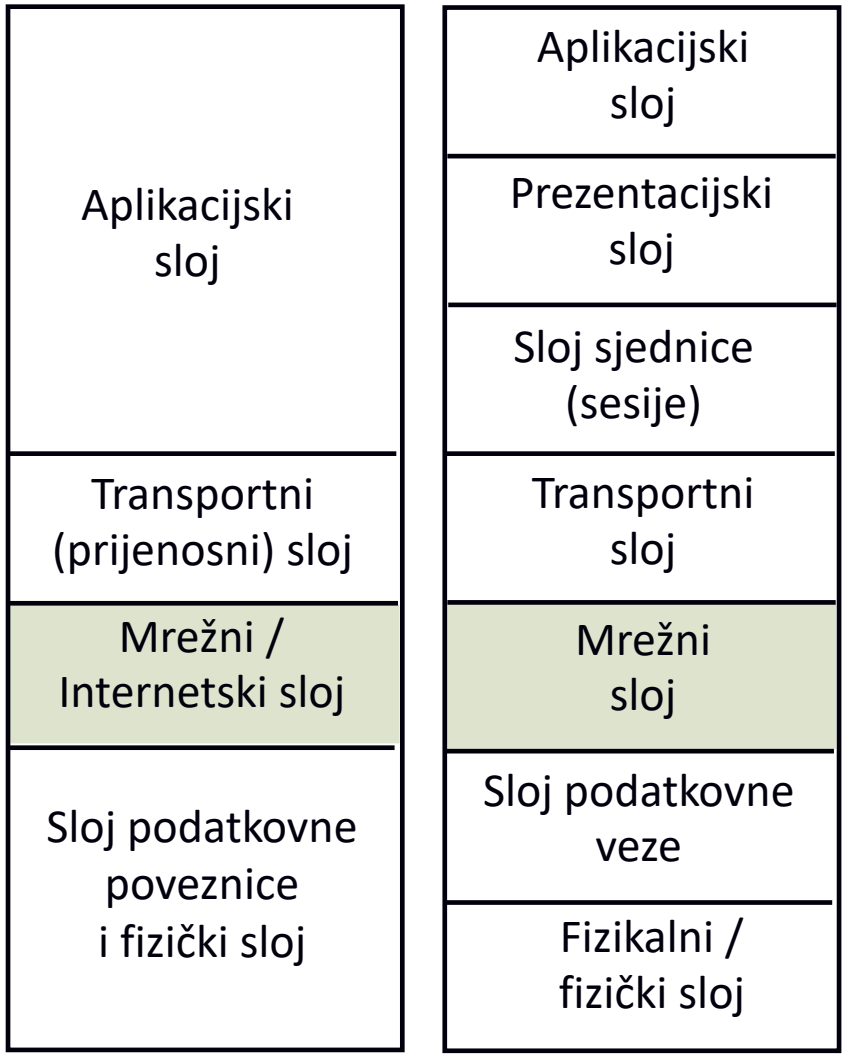
Tekst licencije preuzet je s http://creativecommons.org/.

Sadržaj

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

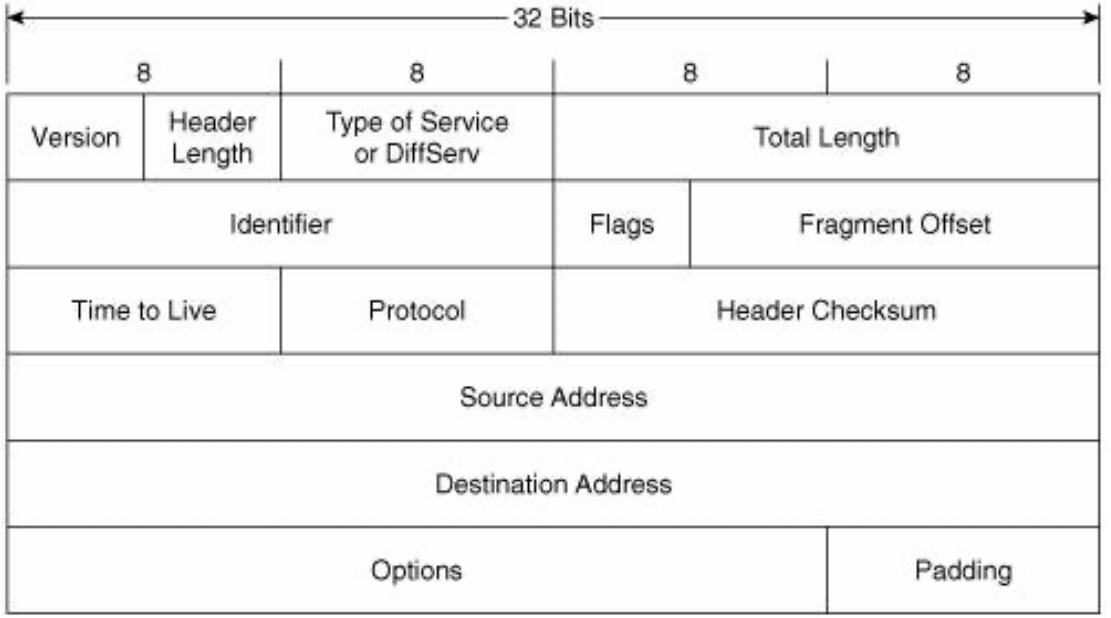
Općenito o mrežnom sloju

- 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!

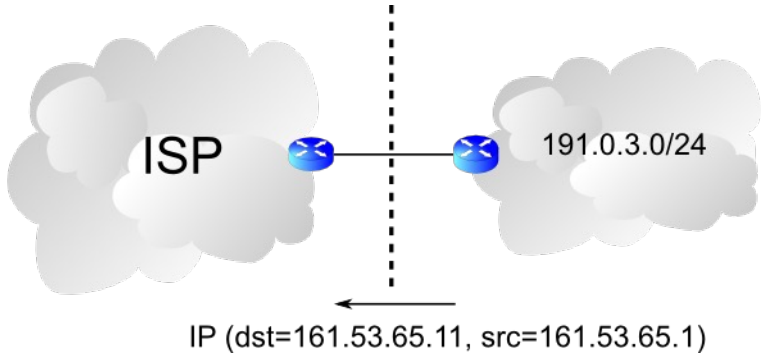


IP zavaravanje (engl. IP spoofing)

- 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
    - Zabrana 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://spoofer.caida.org/summary.php)

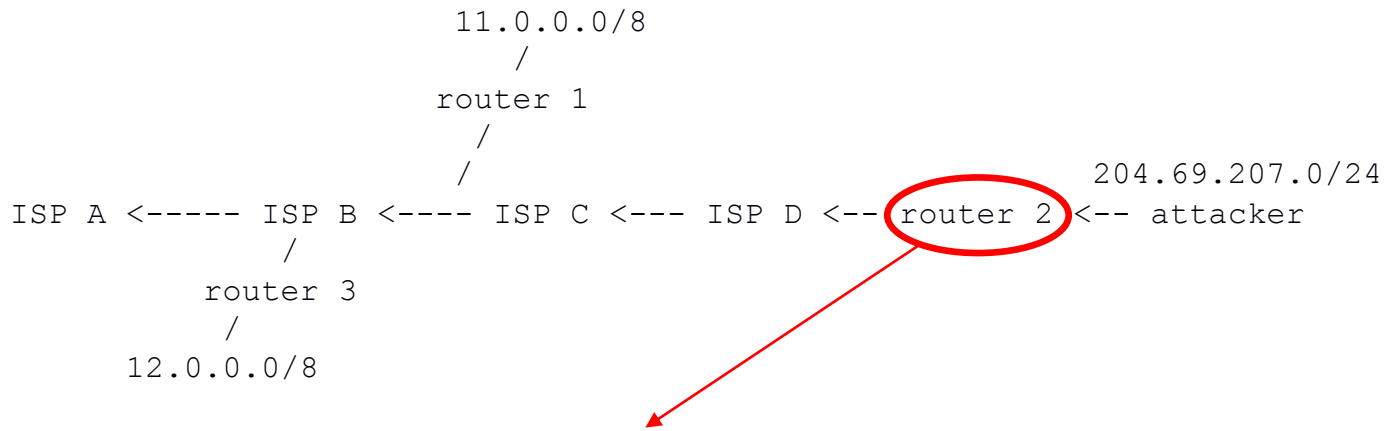
Filtriranje neispravnih izvorišnih adresa

- 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
```

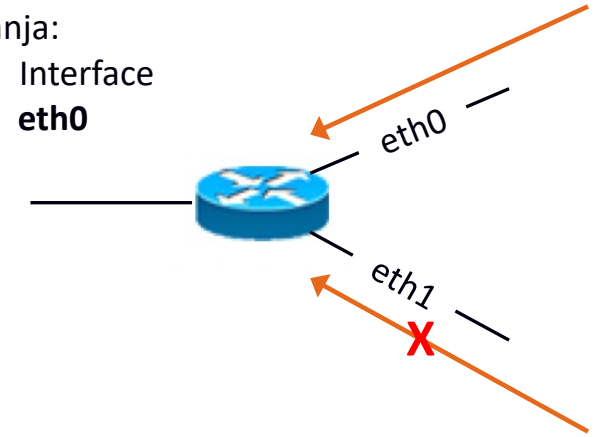
- a napadač (“*attacker*”), za svoju zaštitu, može filtrirati sve dolazne pakete iz Interneta s izvorišnom adresom 204.69.207.0/24

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 kompliciranije kod asimetričnog usmjeravanja (veza na više ISP)

Tablica usmjeravanja:

Destination	Interface
161.53.19.0/24	**eth0**
...	



IP source	IP destination
161.53.19.80/24	...

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

IP fragmentacija - primjeri napada

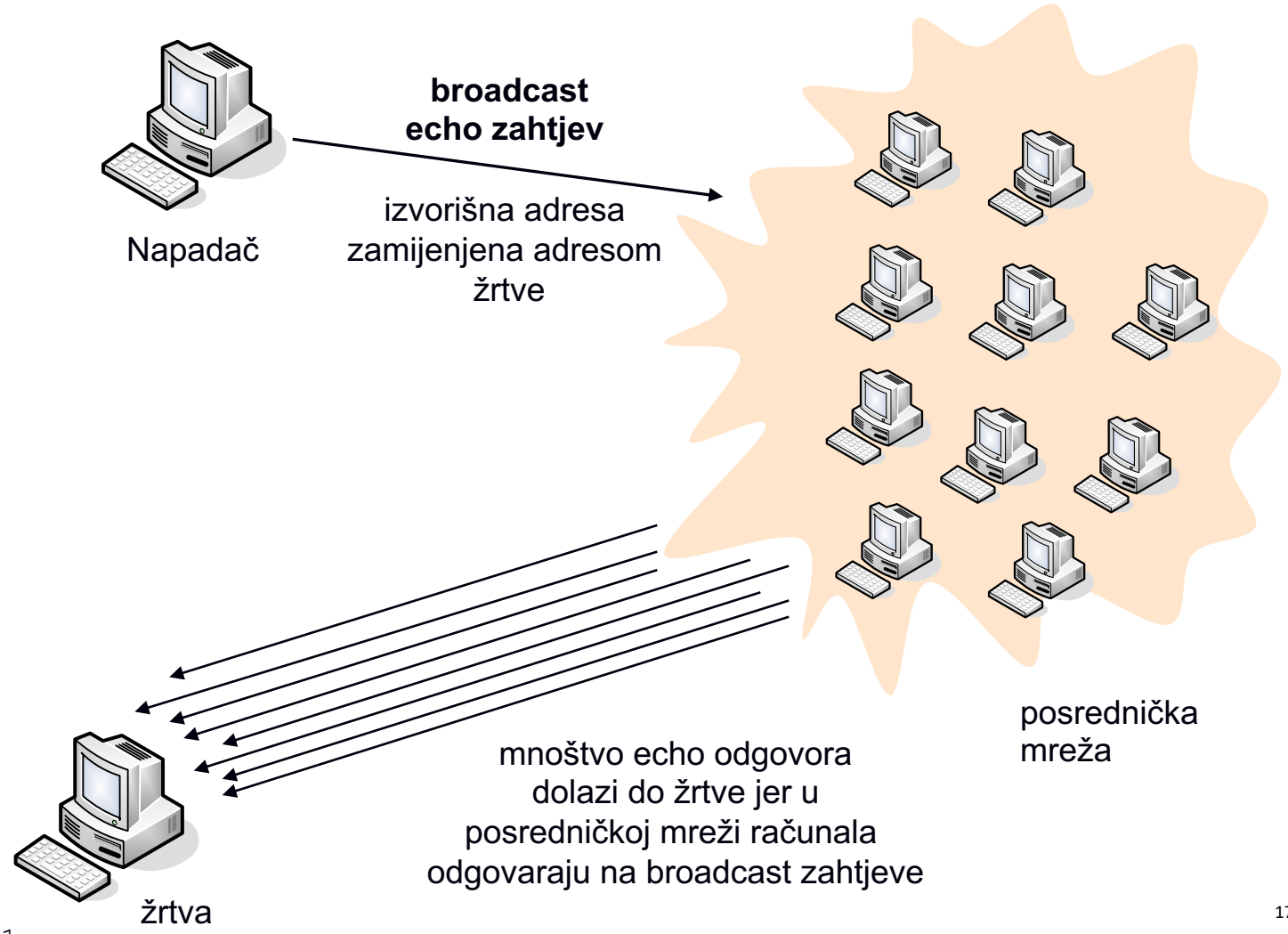
- "*TCP overwrite*"
  - varijacija napada “*teardrop*”
  - nije napad tipa DoS već se pokušava prevariti vatrozid
  - IP datagram se fragmentira, TCP zaglavlje sadrži dozvoljeni port, na primjer 80, pa ga vatrozid propušta
  - neki sljedeći fragment ima „pomak” postavljen na 1 što znači da će port biti 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




```
sysctl net.ipv4.icmp_echo_ignore_broadcasts=1
```

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

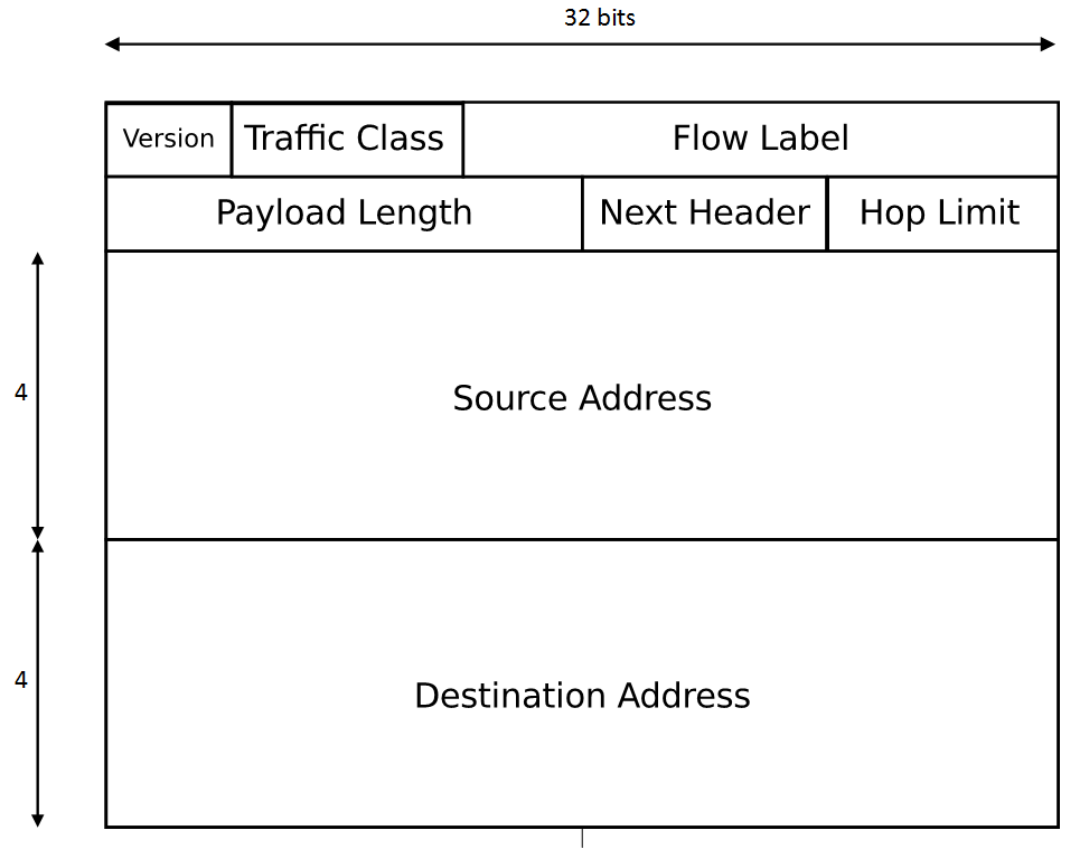
- Zašto uopće spominjati sigurnost protokola IPv6?
  - Na razini RIR-ova IPv4 adrese su iscrpljene te je neminovno uvođenje IPv6
  - Značajni napori da se popularizira i uvede IPv6
- Dosta operacijskih sustava već ima omogućen IPv6
  - Windows OS počevši sa Windows Vista u podrazumijevanoj konfiguraciji 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
  - Pojednostavljeno zaglavlje
  - Fragmentacija se više ne provodi u mrežnom sloju
  - ARP se više ne koristi
  - Automatsko podešavanje mrežnih parametara
- Zaglavlje 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

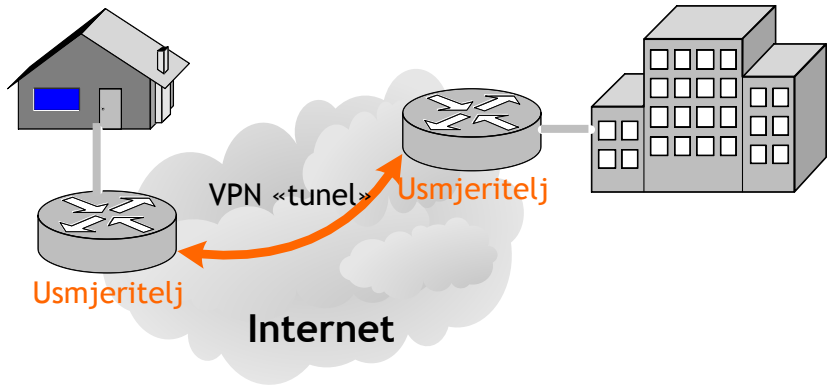
- Virtualne privatne mreže, VPN, „Virtual Private Networks”
  - ista (sigurnosna) politika i performanse kao i privatne mreže realizirane preko infrastrukture WAN
  - sigurni VPN (Secure VPN):
    - **autentifikacija** korisnika/računala, **tajnost** i **integritet** podataka

Virtualne privatne mreže

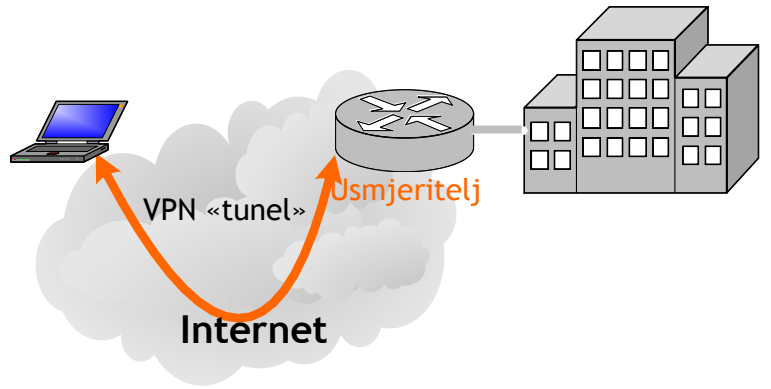
- Virtual Private Networks (VPN)
  - Pojam koji označava stvaranje privatnih mreža nad javnom infrastrukturom Interneta
  - Zamjena za nekadašnje iznajmljivanje linkova, modeme, i slično.
  - Nije specifičnost mrežnog sloja, ali je nužno prenositi IP pakete
- Rješenja za ostvarenje virtualnih privatnih 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

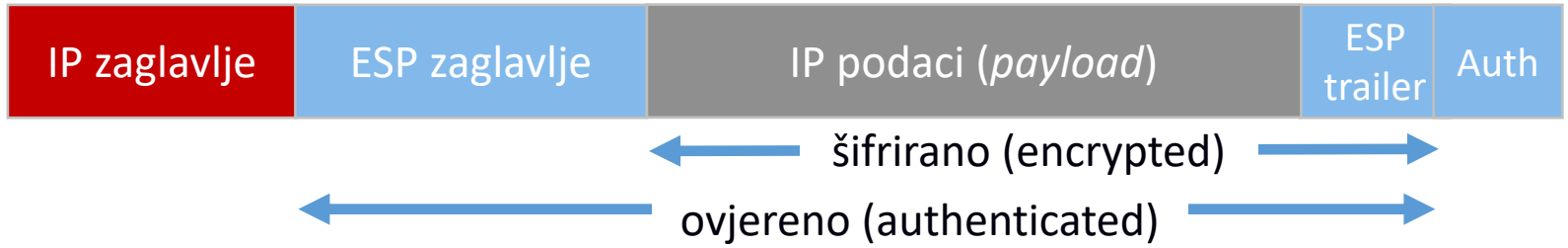
Osnove arhitekture IPsec (2)

- 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

GRE (Generic Routing Encapsulation), protokol: 47

IPsec transportni način



IPsec tunelirani način

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

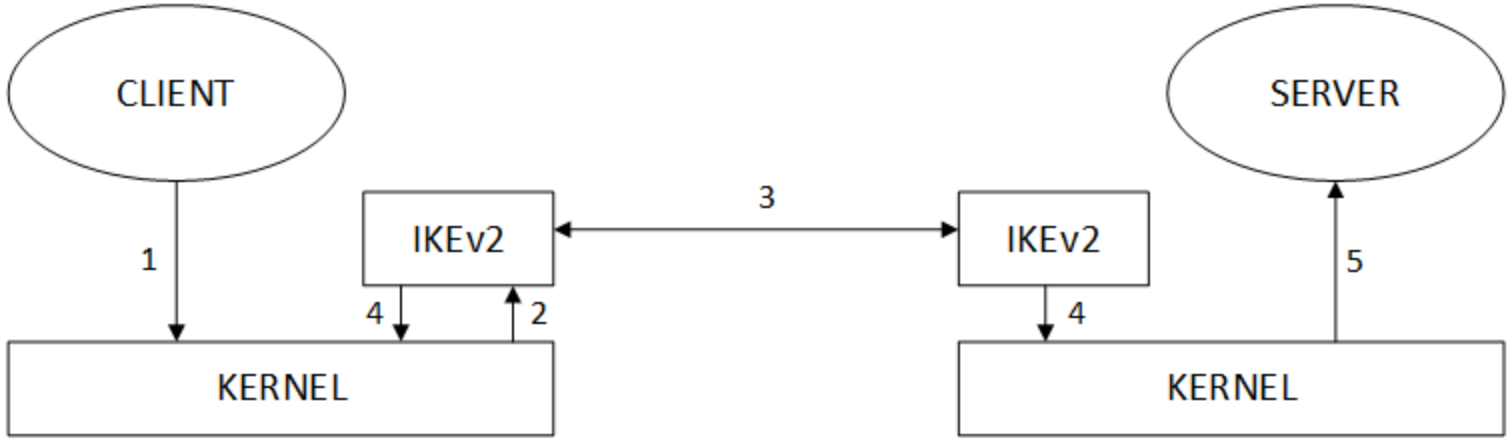
```
161.53.65.225 161.53.65.11
        esp mode=tunnel spi=15702(0x00003d56) reqid=0(0x00000000)
        E: 3des-cbc  31323334 35363738 39303132 31323334 35363738 39303132
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 22 15:52:52 2010                   current: Nov 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 izveden 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
  - izvorišna 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