



SVEUČILIŠTE U ZAGREBU



Fakultet  
elektrotehnike i  
računarstva

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, prerađu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

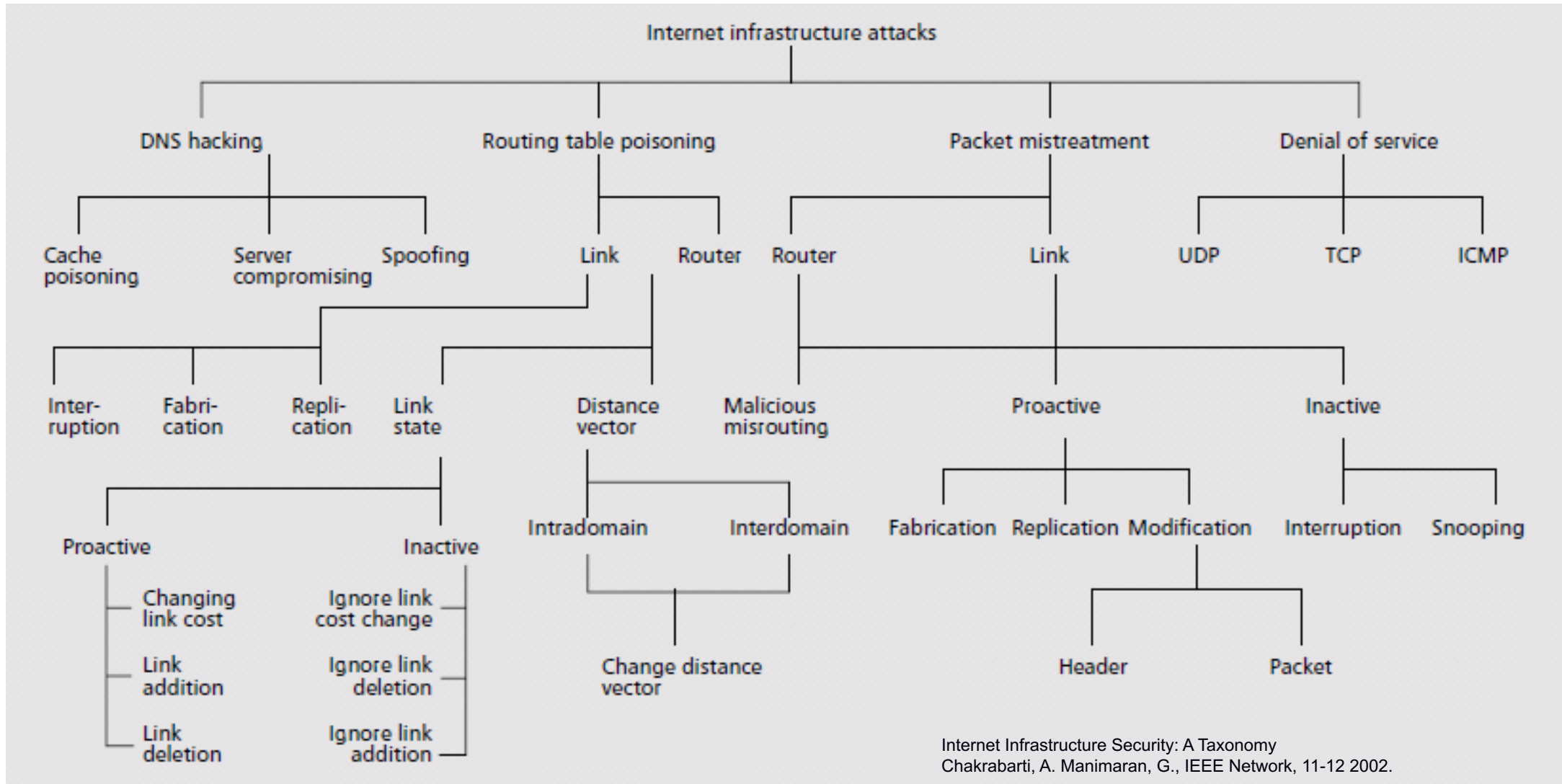


U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci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

# 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 „zapisi resursa” (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

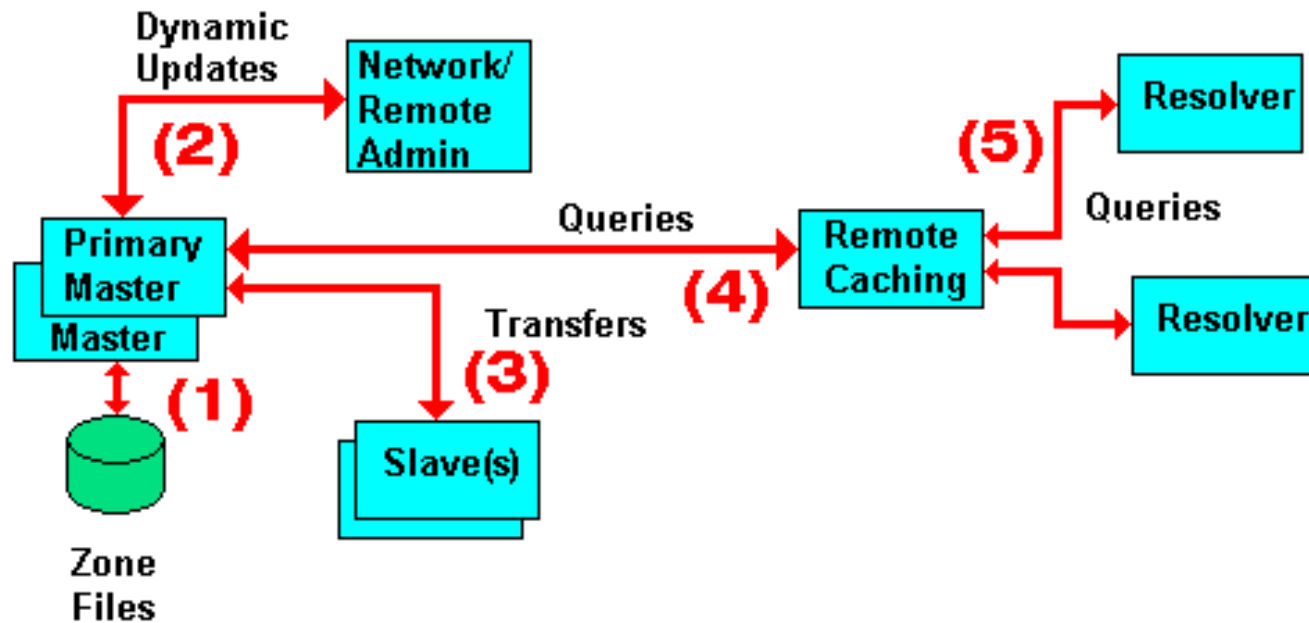
- generičke komponente sustava su
  - klijent, „resolver”, autoritativni poslužitelj, poslužitelj s priručnom memorijom
- u sustavu DNS fiksirani su samo korijenski poslužitelji (engl. root servers)
  - svako računalo dolazi s popisom IP adresa tih poslužitelja
  - svi ostali poslužitelji se dinamički 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 prerušavanje (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 kompletnu 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

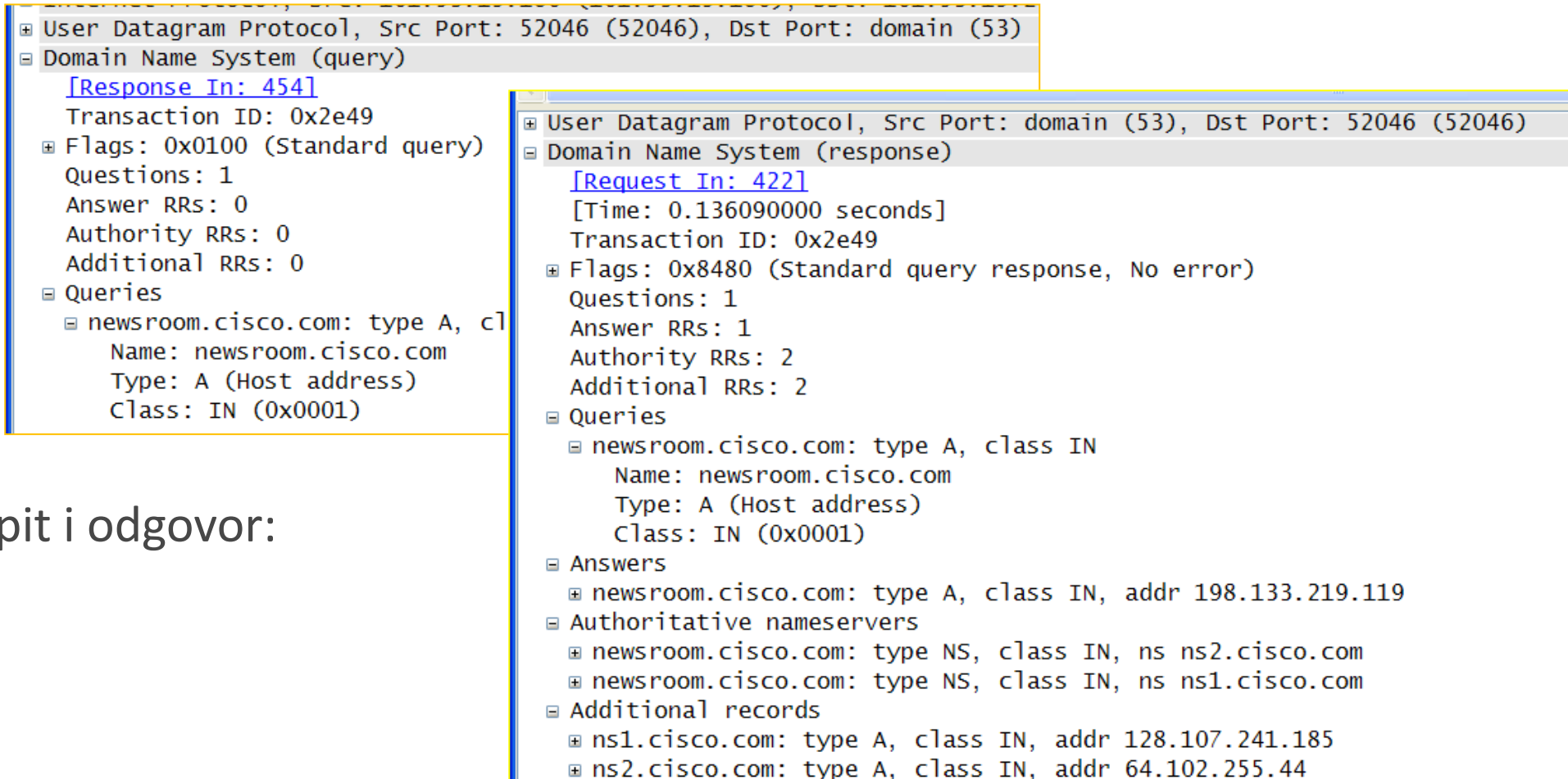
# Prijetnje sustavu DNS (3)

- „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”



The image displays two Wireshark packet capture screenshots. The left screenshot shows a DNS query (Transaction ID: 0x2e49) from a client (Src Port: 52046) to a server (Dst Port: domain (53)). The query is for newsroom.cisco.com, type A, class IN. The right screenshot shows the corresponding DNS response (Transaction ID: 0x2e49) from the server (Src Port: domain (53)) to the client (Dst Port: 52046). The response includes the requested record for newsroom.cisco.com (type A, class IN, address 198.133.219.119) and additional records for authoritative nameservers ns1.cisco.com and ns2.cisco.com.

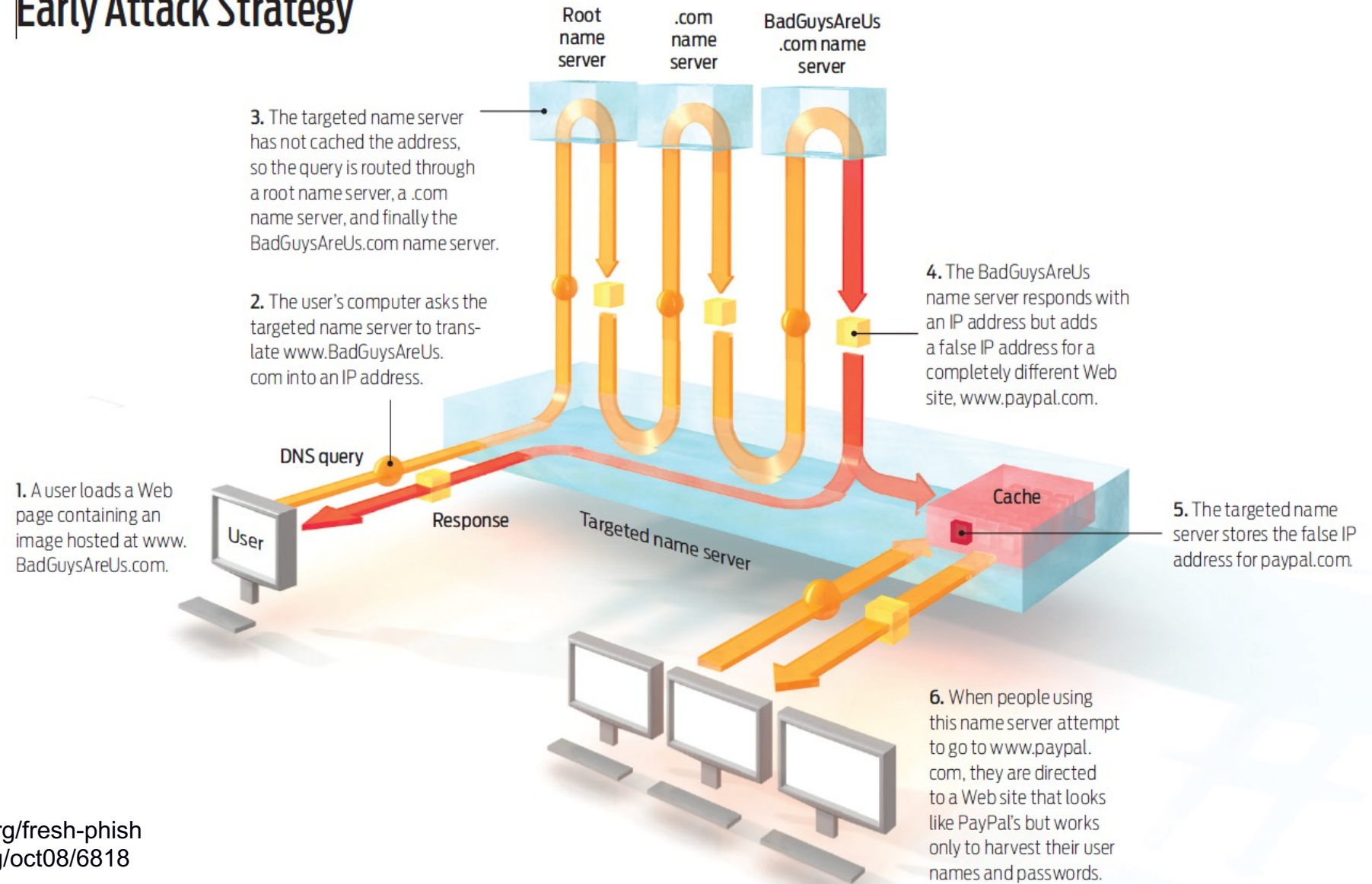
```
⊕ User Datagram Protocol, Src Port: 52046 (52046), Dst Port: domain (53)
⊖ Domain Name System (query)
  [Response In: 454]
  Transaction ID: 0x2e49
  ⊕ Flags: 0x0100 (Standard query)
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ⊖ Queries
    ⊖ newsroom.cisco.com: type A, class IN
      Name: newsroom.cisco.com
      Type: A (Host address)
      Class: IN (0x0001)

⊕ User Datagram Protocol, Src Port: domain (53), Dst Port: 52046 (52046)
⊖ Domain Name System (response)
  [Request In: 422]
  [Time: 0.136090000 seconds]
  Transaction ID: 0x2e49
  ⊕ Flags: 0x8480 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
  ⊖ Queries
    ⊖ newsroom.cisco.com: type A, class IN
      Name: newsroom.cisco.com
      Type: A (Host address)
      Class: IN (0x0001)
  ⊖ Answers
    ⊕ newsroom.cisco.com: type A, class IN, addr 198.133.219.119
  ⊖ Authoritative nameservers
    ⊕ newsroom.cisco.com: type NS, class IN, ns ns2.cisco.com
    ⊕ newsroom.cisco.com: type NS, class IN, ns ns1.cisco.com
  ⊖ Additional records
    ⊕ ns1.cisco.com: type A, class IN, addr 128.107.241.185
    ⊕ ns2.cisco.com: type A, class IN, addr 64.102.255.44
```

- DNS upit i odgovor:

# DNS Cache poisoning

## Early Attack Strategy

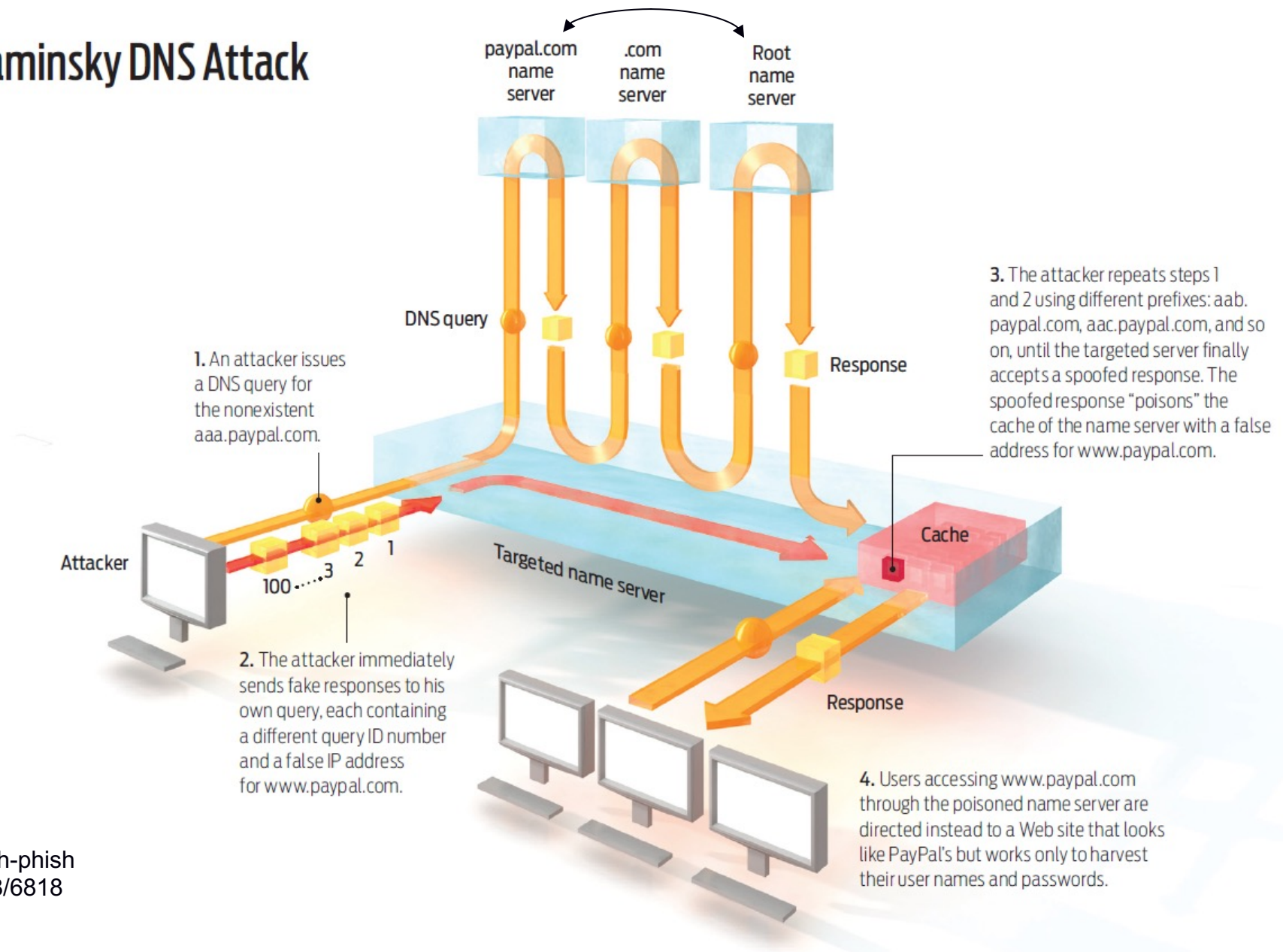


Kopirano iz:  
<https://spectrum.ieee.org/fresh-phish>  
<http://spectrum.ieee.org/oct08/6818>



# 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.jsf-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 prihvaća 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 (".") potpisan!

# 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 spreman 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 .
jxhECtLYokMAZeUYB1F3KFnlZQJmdBgWK611UwJW1cCdZ+6XyCxnOdp TQDIyfUX6T84cbVI05KgSq70+Zxm3mZuUKZPNUb5NFmoD9RnfJaHH4cX
19EHSdayTvAwbSvnqh6YKJDk5bp3ZkFv+7J8UBOPv4Cdsl63/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 raspodjelu 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 odabranih 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

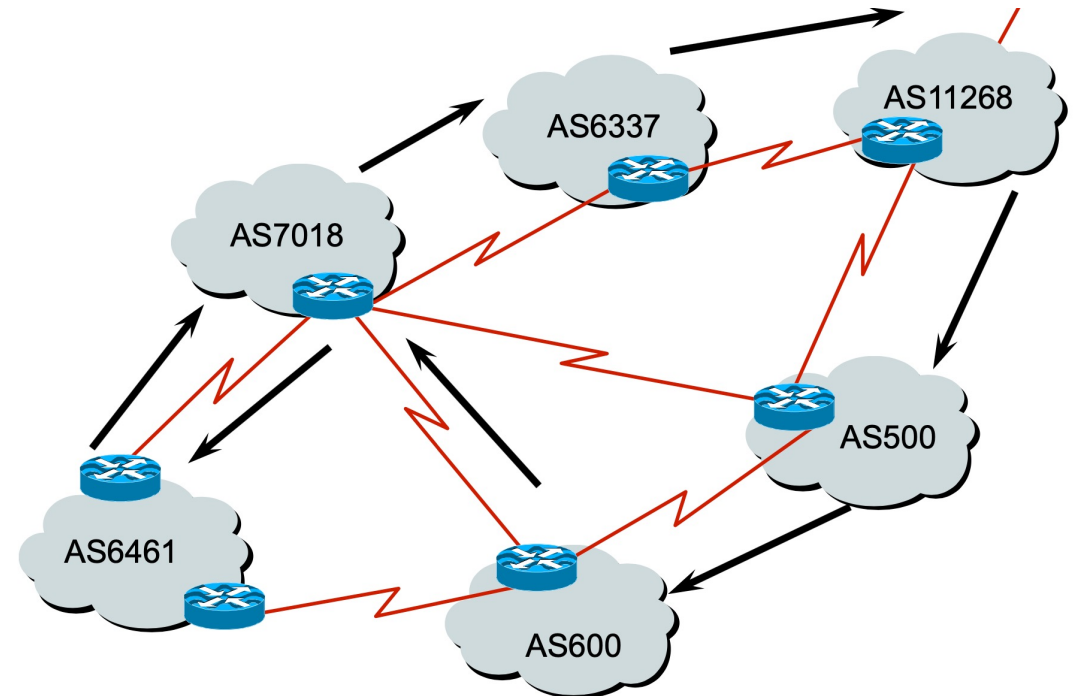
# Path Vector Protocol

- 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 „asdot”)
  - 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 oglašanih 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 *speaker*a 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 ...
  - krivotvorenje (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/>