



UDP (User Datagram Protocol)
QUIC
TLS (Transport Layer Security)

PROTOKOL ZA PRENOS KORISNIČKIH DATAGRAMA

UDP (User Datagram Protocol)

Osobine UDP-a

- ◆ UDP je jednostavan protokol transportnog nivoa, orijentisan na poruke (message oriented).
- ◆ Ne podržava uspostavu veze (UDP je connectionless protokol)
- ◆ Sadrži minimum tipičnih protokol mehanizama
- ◆ Standard je u RFC 768

Mehanizmi koje sadrži UDP

- ◆ Kontrolna suma (checksum) da bi se proverio integritet podataka
- ◆ Broj prolaza (porta) da bi se adresirale različite aplikacije na računaru

Mehanizmi koje NE sadrži UDP

- ◆ Pouzdanost
- ◆ Nema garancije isporuke
- ◆ Nema garancije očuvanja redosleda datagrama
- ◆ Nema zaštite od pojave višestrukih (dupliciranih) datagrama
- ◆ Nema upravljanja tokom

Još neke osobine UDP

- ◆ Nema unutrašnje stanje (UDP je stateless)
- ◆ Podržava višeznačno upućivanje (multicast)
- ◆ Jednostavan je

Struktura UDP datagrama

- ◆ Zaglavlje + sekcija podataka
- ◆ Zaglavlje sadrži 4 polja, svako po dva bajta dužine, u sledećem redosledu: izvorišni prolaz, odredišni prolaz, dužina datagrama, kontrolna suma
- ◆ U IPv4 izvorišni prolaz i kontrolna suma su opcioni
- ◆ U IPv6 samo je izvorišni prolaz opcioni

- ◆ Maksimalna dužina UDP datagrama u IPv4 je 65507 bajtova, što je $65535 - 8$ (UDP zaglavlje) $- 20$ (IPv4 zaglavlje)
- ◆ Za izračunavanje kontrolne sume se koristi pseudo zaglavlje

Prolazi

- ◆ Adrese transportnog nivoa
- ◆ Multipleksiranje aplikacija
- ◆ 16-bitne celobrojne vrednosti: 0-65535
- ◆ IANA je podelila ovaj opseg na tri dela:
 - 0-1023 – well known usluge
 - 1024-49151 – usluge registrovane kod IANA
 - 49152-65535 – prolazi koji se mogu slobodno koristiti, efemerni (ephemeral) prolazi koji se dinamički dodeljuju

Primene UDP protokola

- ◆ Jednostavnost UDP protokola i odsustvo nekih složenih mehanizama koji postoje u TCP (na primer retransmisije i kašnjenja koje unose) ga čine pogodnim za aplikacije u realnom vremenu kao što su prenos glasa preko Interneta (VoIP), prenos multimedijalnog toka podataka (streaming) i igre na mreži
- ◆ Za prenos audia i videa je manji problem povremeni gubitak paketa nego kašnjenje koje unose TCP mehanizmi retransmisije izgubljenih paketa

Primene UDP protokola II

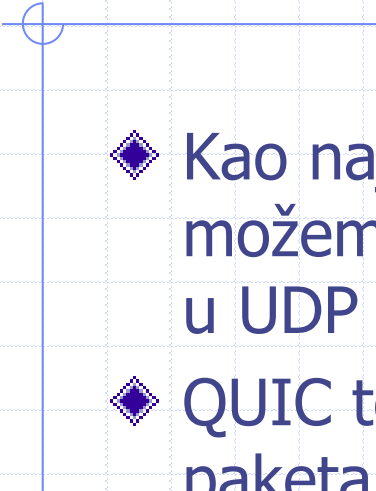
- ◆ QUIC je noviji transportni protokol zasnovan na UDP
- ◆ Neke važne Internet aplikacije i protokoli koriste UDP: DNS, SNMP, RIP i DHCP
- ◆ Jednostavnost UDP takođe omogućuje da potrebni mehanizmi (pouzdanost na primer) budu implementirani u aplikaciji



QUIC

QUIC

- ◆ Transportni protokol
- ◆ Izgovara se quick
- ◆ U upotrebi je od 2012.
- ◆ Razvoj protokola je u prvoj fazi išao u okviru Google, kasnije je IETF preuzeo

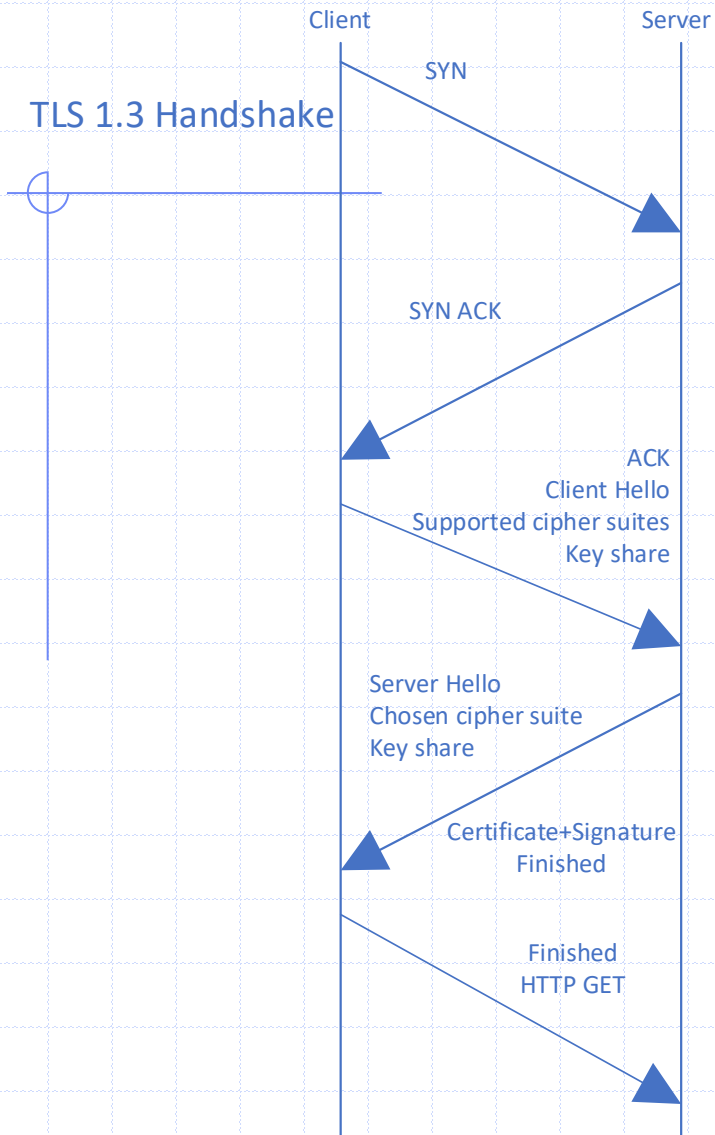
- 
- ◆ Kao najjednostavniji mada ne i najtačniji opis QUIC možemo reći da je to enkriptovani TCP koji se prenosi u UDP datagramu.
 - ◆ QUIC tok u mreži izgleda kao dvosmerni niz UDP paketa sa šifrovanim sadržajem.

- ◆ QUIC koristi kombinaciju dva broja kao identifikator veze, pri čemu svaka strana bira po jedan broj.
- ◆ Ovaj identifikator veze omogućuje adresiranje kada dođe do promene IP adrese ili prolaza neke od strana u komunikaciji
- ◆ Ovo omogućuje da se očuva veza kada dođe do promene u adresi ili prolazu, na primer zbog NAT-a (moguće kod interakcije UDP i NAT ako je UDP komunikacija pauzirana duže nego što je vremenska kontrola na NAT) ili prelaska sa mobilne mreže na WiFi.

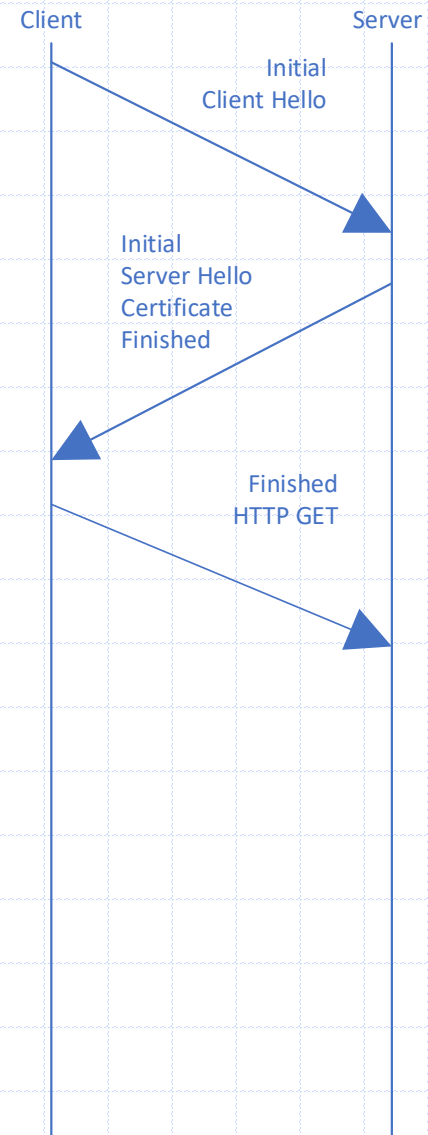
QUIC povezivanje

- ◆ Tipična uspostava veze za TCP+TLS podrazumeva razmenu 5 poruka, dok je QUIC uspostava u 3 koraka, što je ušteda od jednog RTT, što je od značaja za kratkotrajne veze.

TLS 1.3 Handshake



QUIC Handshake



Osobine QUIC-a

- ◆ Na QUIC vezi se razmenjuju paketi. Svaki paket je označen jednoznačno u 62-bitnom prostoru. Zanovljeni paket dobija novi broj. (no ACK ambiguity)
- ◆ QUIC paketi se zasebno enkriptuju tako da dekripcija jednog paketa ne zavisi od drugih.
- ◆ QUIC prijemnik potvrđuje najveći jedinstveni broj primljenog paketa, zajedno sa listom od maksimalno 256 kontinualnih blokova paketa, ako ima gubitaka.
- ◆ To je prednost u odnosu na TCP gde Selective ACK omogućuje maksimalno 3 takva bloka.

QUIC tokovi

- ◆ QUIC veza se sastoji od tokova i dve strane u komunikaciji mogu da se dogovore o podeli prenosnog opsega između tokova, kao i o prioritetima tokova.
- ◆ QUIC tok ima svoj identifikator i po osobinama je sličan TCP toku.

QUIC datagrami

- ◆ Pored tokova koji su pouzdani, QUIC nudi i mogućnost datagrama, koji su šifrovani, ali nepouzdani.

QUIC okviri

- ◆ QUIC paketi sadrže jedan ili više okvira.
- ◆ Postoji oko 20 vrsta okvira.

Primene QUIC

- ◆ HTTP/3 je predloženi standard iz 2022, objavljen u RFC 9114, koji je zasnovan na QUIC, za razliku od HTTP/1.1 i HTTP/2 koji su zasnovani na TCP i TLS.

Naziv

- ◆ Prvobitno je QUIC bio akronim za Quick UDP Internet Connections, ali prema IETF QUIC je naziv



Transport Layer Security - TLS

Namena

- ◆ TLS je kriptografski protokol za zaštitu komunikacija u računarskoj mreži
- ◆ Danas ga koriste različite aplikacije: elektronska pošta, instant poruke, VoIP ali je najpoznatiji kao protokol za zaštitu veb saobraćaja (HTTPS)
- ◆ Zaštita komunikacija se odnosi na obezbeđivanje integriteta, privatnosti i autentikacije korišćenjem kriptografije

Mesto u protokol steku

- ◆ Nalazi se između aplikacije i transportnog nivoa, i obavlja neke funkcije prezentacionog nivoa, pa ga možemo svrstati u taj nivo
- ◆ Međutim aplikacije koriste TLS kao da je on još jedan transportni protokol, pa to unosi malu zabunu

Korišćenje TLS

- ◆ Aplikacije tipično koriste poseban prolaz za komunikaciju zaštićenu TLS-om
- ◆ Tako kod veb saobraćaja, port 80 se koristi za nezaštićeni HTTP saobraćaj, a port 443 za HTTPS saobraćaj zaštićen TLS-om

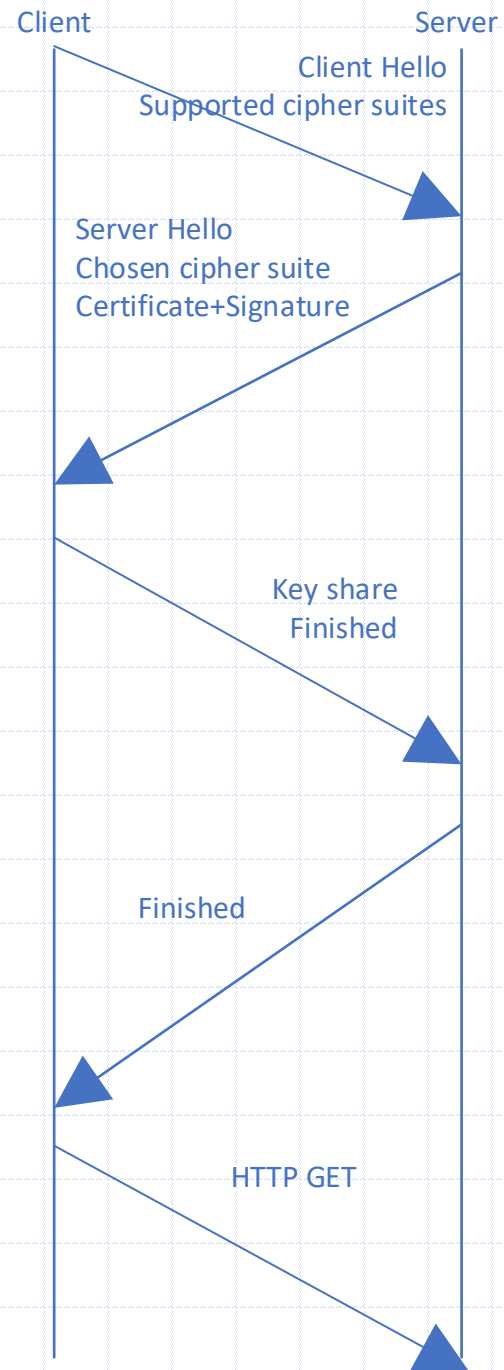
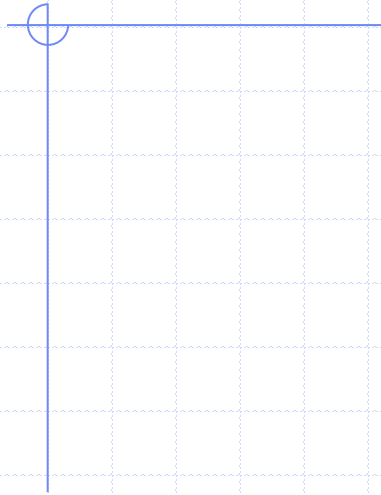
Mehanizam zaštite

- ◆ Klijent i poslužilac pregovaraju i uspostavljaju zaštićenu vezu
- ◆ U početnoj fazi koriste asimetrični krypto sistem kojim formiraju deljeni ključ za zaštitu sesije
- ◆ Nadalje koriste deljeni ključ sa simetričnim krypto sistemom za zaštitu komunikacije na uspostavljenoj vezi

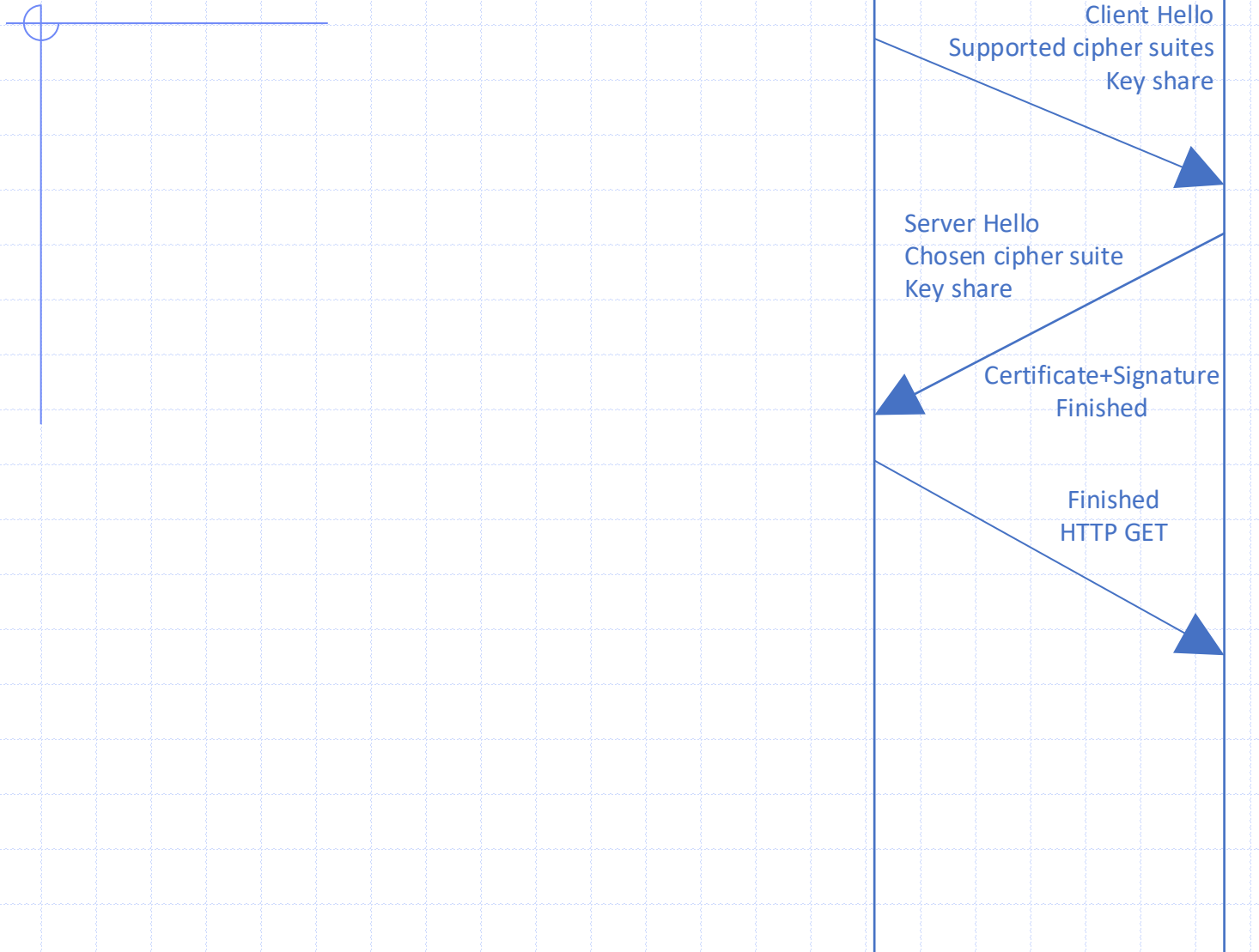
Uspostava veze

- ◆ Započinje je klijent koji se povezuje sa poslužiocem i šalje listu kriptó algoritama koje podržava
- ◆ Iz te liste poslužilac bira kriptó algoritam i heš funkciju koju će koristiti i o tome obaveštava klijenta
- ◆ Poslužilac prosleđuje klijentu svoj digitalni sertifikat koji sadrži javni ključ poslužioca
- ◆ Klijent proverava da li je sertifikat važeći
- ◆ Klijent generiše slučajan broj i šifruje ga javnim ključem poslužioca, što poslužilac može da dešifruje svojim tajnim ključem
- ◆ Obe strane koriste ovaj slučajan broj da izgenerišu ključ za zaštitu sesije

TLS 1.2 Handshake



TLS 1.3 Handshake



Osobine zaštićene veze

- ◆ Privatnost je obezbeđena simetričnim krypto sistemom koji koristi ključe sesije
- ◆ Za autentikaciju se koristi asimetrični krypto sistem
- ◆ Proverava se integritet primljene poruke

Istorija

- ◆ TLS je nastao na osnovi SSL protokola (Secure Sockets Layer) razvijenog od strane kompanije Netscape
- ◆ TLS 1.0 je objavljen u RFC 2246 1999. godine
- ◆ Trenutna verzija je TLS 3.0 objavljena u RFC 8446 2018. godine

Tajnost unapred

- ◆ Forward secrecy
- ◆ Kod sistema koji nema ovu osobinu, ukoliko dođe do razbijanja tajnog ključa biće moguće dešifrovati sve sesije koje su u prošlosti koristile taj ključ, ako su snimljene
- ◆ Kod sistema koji podržava ovu mogućnost, sadržaj sesije je bezbedan i ako u budućnosti bude razbijen tajni ključ
- ◆ TLS može obezbediti tajnost unapred, u zavisnosti od dogovorenog krypto algoritma na vezi
- ◆ Gmail koristi ovu osobinu

Presretanje TLS veze

- ◆ Praksa za zaštitu mreža od neželjenih komunikacija
- ◆ Koristi se transparentni posrednik (transparent proxy) koji prekida uspostavu TLS veze sa poslužiocem, analizira HTTP saobraćaj, i uspostavlja novu TLS vezu sa poslužiocem

Datagram Transport Layer Security, DTLS

- ◆ Protokol zasnovan na TLS čija je namena zaštita datagramskog saobraćaja