SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

TLS

Creative Commons

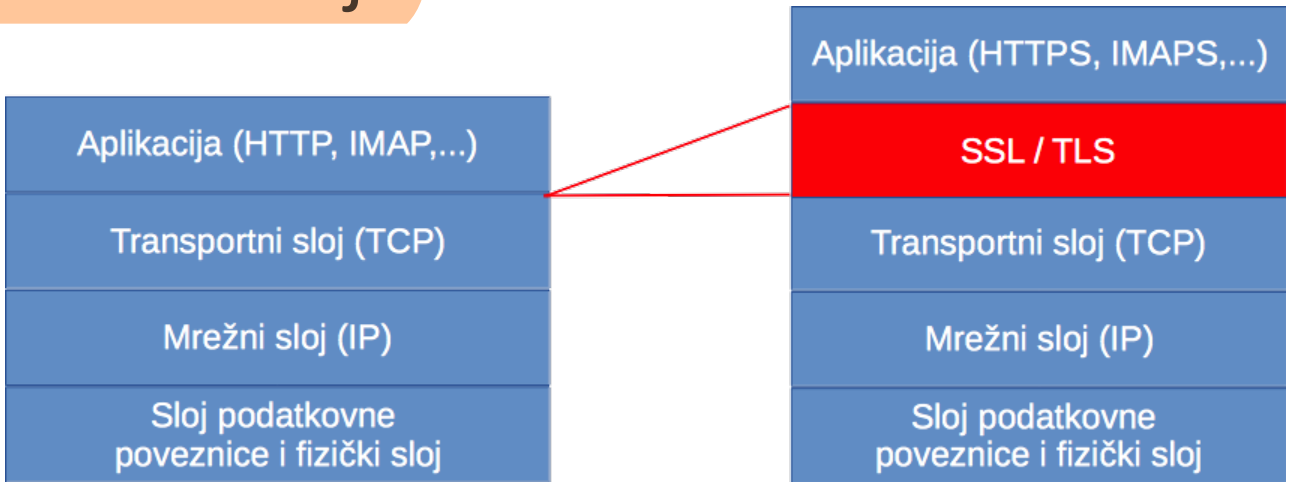
- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način 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 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/.

Model prijetnje

- Protokol TLS služi za zaštitu komunikacije
- Pretpostavke:
  - 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 presiječe 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]

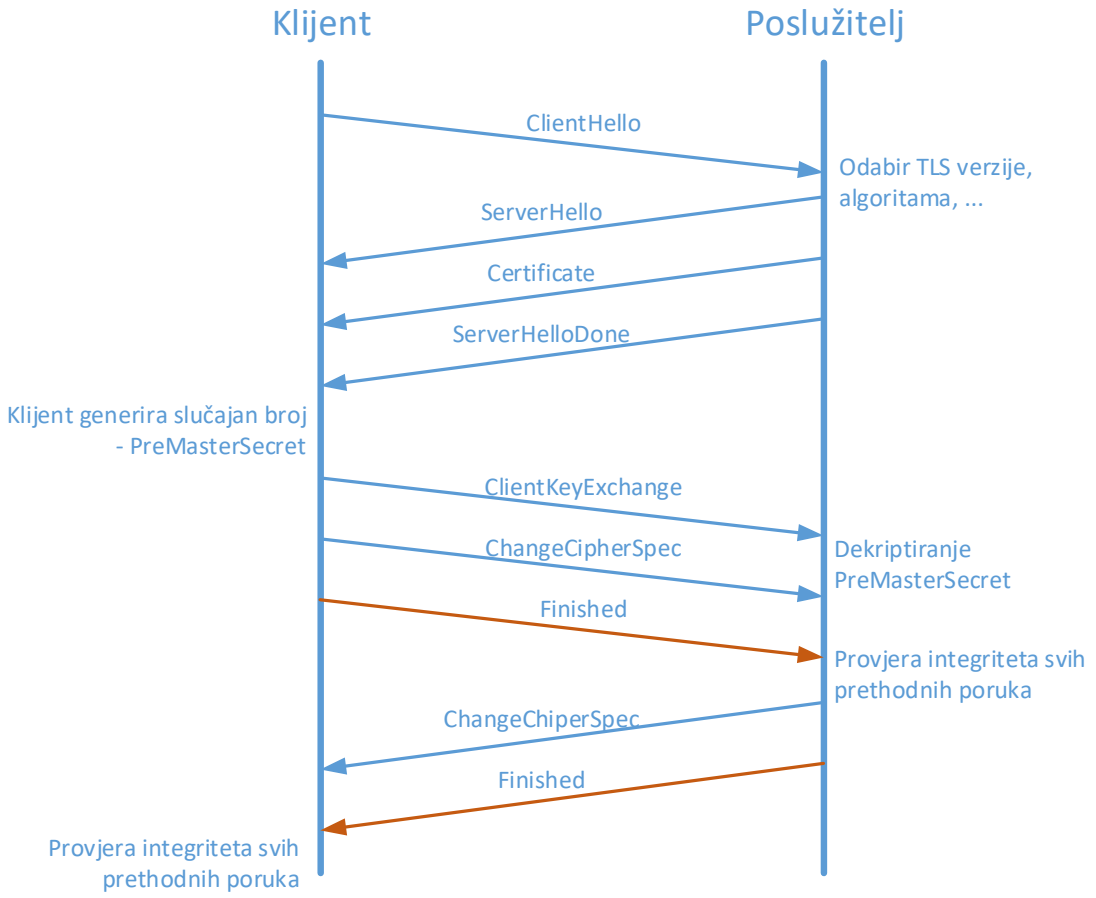
. . .

HTTP + TLS

- Najčešća upotreba TLS-a: HTTPS
  - Korisnik na klijentskoj strani (u pregledniku) zahtijeva 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

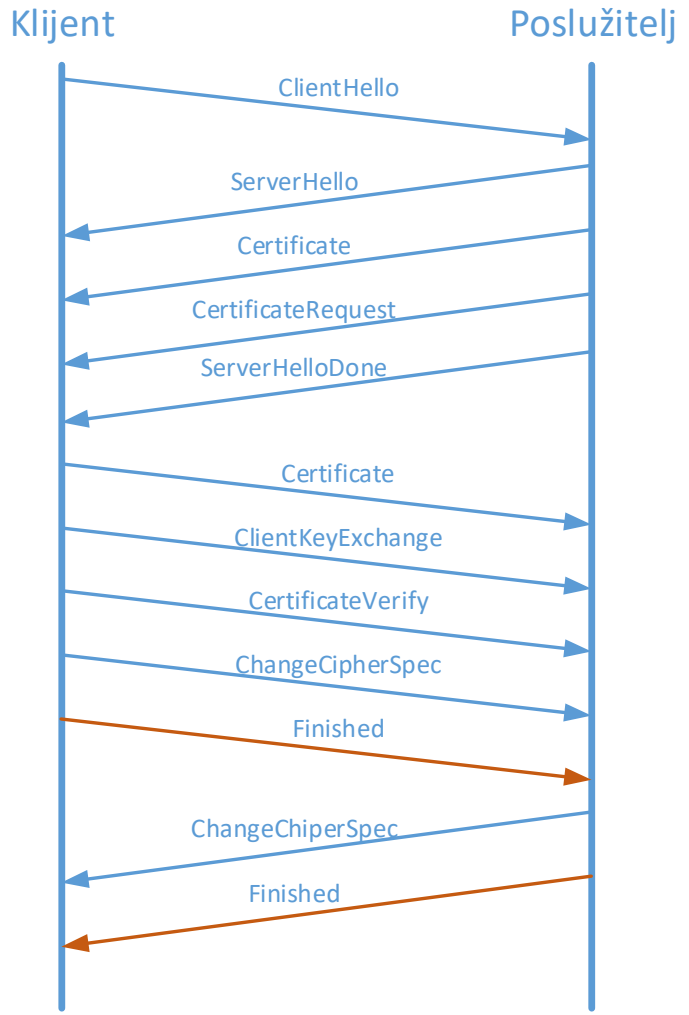
- Potvrda identiteta poslužitelja i zaštita tajnosti i autentičnosti komunikacije
- Izvršava se nad protokolom TCP
  - Postoji i varijanta nad protokolom UDP – DTLS (prvenstveno definiran zbog VoIP-a)
    - UDP varijanta je gotovo identična TCP varijanti



- 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 zlućudnog 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
  - Prisiljava 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
  - nazive 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 cerifikata 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!