PANEVROPSKI UNIVERZITET “APEIRON”

U BANJOJ LUCI

FAKULTET INFORMACIONIH TEHNOLOGIJA

Seminarski rad iz predmeta „Zaštita računarskih i poslovnih sistema“

Kriptoanalitički napadi i problemi koji se odnose na SSL protokol

Profesor

Prof. dr Nemanja Maček

Kandidat

Ivan Pavlović

Banja Luka, 28. mart 2025

Sadržaj

Apstrakt:

Secure Sockets Layer (SSL)[1] i njegov nasljednik Transport Layer Security (TLS)[2] ključni su protokoli za osiguranje sigurnosti podataka na internetu. Međutim, unatoč širokoj primjeni, SSL/TLS je izložen brojnim kriptoanalitičkim napadima koji iskorištavaju slabosti u dizajnu ili implementaciji. Ovaj rad analizira najznačajnije prijetnje, uključujući Man-in-the-Middle (MITM)[3] napade, BEAST[4], POODLE[5] i Heartbleed[6], te probleme poput zastarjelih enkripcionim sistema i loše konfiguracije servera. Također se razmatraju metode zaštite, kao što su primjena TLS 1.3, ispravna konfiguracija enkriptovanja i redovna ažuriranja. Cilj rada je ukazati na ranjivosti SSL/TLS protokola te istaknuti najbolje prakse za njihovo ublažavanje kako bi se osigurala sigurna online komunikacija.

Ključne riječi: *SSL/TLS, kriptoanalitički napadi, sigurnost podataka, zaštita protiv napada*

[1] SSL (Secure Sockets Layer) - protokol za enkriptovanu komunikaciju
[2] TLS (Transport Layer Security) - nasljednik SSL-a, sa poboljšanim sigurnosnim mehanizmima
[3] MITM (Man-in-the-Middle) - napad gdje napadač presreće komunikaciju
[4] BEAST (Browser Exploit Against SSL/TLS) - napad na CBC način u TLS 1.0
[5] POODLE (Padding Oracle On Downgraded Legacy Encryption) - iskorištavanje SSL 3.0 ranjivosti
[6] Heartbleed - ranjivost u OpenSSL biblioteci koja omogućuje curenje memorije

1 Uvod

U vremenu digitalizacije i sve veće zavisnosti od online komunikacije, zaštita podataka postaje ključni aspekt modernog društva. Secure Sockets Layer (SSL) i njegov nasljednik Transport Layer Security (TLS) predstavljaju temeljne sigurnosne protokole koji omogućavaju autentičnu, privatnu i integritetom zaštićenu komunikaciju preko interneta. Ovi protokoli se široko koriste u web pregledačima, bankovnim aplikacijama, e-pošti i drugim servisima koji zahtijevaju sigurnu razmjenu informacija. Međutim, unatoč svojoj kritičnoj ulozi, SSL/TLS protokoli nisu imuni na sigurnosne prijetnje.

Kriptoanalitički napadi na SSL/TLS protokole predstavljaju ozbiljan izazov za informacionu sigurnost. Tokom godina, istraživači su otkrili brojne ranjivosti u dizajnu i implementaciji ovih protokola, što je dovelo do razvoja različitih eksploatacija poput POODLE, BEAST, Heartbleed i MITM napada. Ovi napadi iskorištavaju slabosti u kriptografskim algoritmima, greške u implementaciji ili zastarjele verzije protokola, što može rezultirati krađom osjetljivih podataka, lažnim predstavljanjem ili čak potpunim kompromitovanjem sistema.

Cilj ovog rada je analizirati najznačajnije kriptoanalitičke napade i probleme vezane za SSL/TLS protokole, te predložiti odgovarajuće mjere zaštite. Rad će se fokusirati na tehničke aspekte napada, njihove posljedice i metode prevencije kroz primjenu najnovijih sigurnosnih standarda. Kroz sistematski pregled postojećih ranjivosti i odbrambenih mehanizama, rad nastoji pružiti uvid u aktuelne izazove u održavanju sigurne online komunikacije.

Ova tema je posebno relevantna u kontekstu sve većeg broja sajber napada i rastućih zahtijeva za zaštitom privatnosti. Razumijevanje SSL/TLS ranjivosti i načina njihovog ublažavanja ključno je za sve koji rade u oblasti informacione sigurnosti, kao i za krajnje korisnike koji žele osigurati svoju online sigurnost.

2 Osnove SSL/TLS protokola

SSL (Secure Sockets Layer) i TLS (Transport Layer Security) predstavljaju kriptografske protokole dizajnirane za osiguranje komunikacije preko računarskih mreža. Ovi protokoli omogućavaju autentifikaciju, enkripciju i integritet podataka koristeći kombinaciju asimetrične i simetrične kriptografije, hash funkcija i digitalnih sertifikata.

2.1 Istorija razvoja SSL/TLS protokola

„Razvoj SSL (Secure Sockets Layer) i TLS (Transport Layer Security) protokola započeo je devedesetih godina prošlog vijeka kao odgovor na rastuću potrebu za bezbjednom komunikacijom na internetu. Prvu verziju SSL-a (SSL 1.0) razvila je kompanija Netscape 1994. godine, ali nikada nije objavljena zbog ozbiljnih bezbjednosnih propusta. Već 1995. godine, Netscape je izbacio SSL 2.0, koji je ubrzo postao industrijski standard uprkos određenim bezbjednosnim slabostima“ [1].

Godine 1996. uveden je SSL 3.0, koji je donio značajna poboljšanja u bezbjednosti, uključujući jače enkripcione algoritme i bolji mehanizam za pregovaranje parametara veze. Međutim, i SSL 3.0 je kasnije pokazao ranjivosti, poput POODLE napada (2014), što je dovelo do njegovog postepenog napuštanja.

„Kako bi se prevazišle ograničenosti SSL-a, Internet Engineering Task Force (IETF)[7] standardizovao je TLS 1.0 1999. godine kao nasljednika SSL 3.0. TLS 1.0 je zadržao sličnu strukturu, ali sa unapređenim bezbjednosnim mehanizmima. Kasnije verzije (TLS 1.1 - 2006, TLS 1.2 - 2008, i TLS 1.3 - 2018) uklonile su zastarjele enkripcije i uvele moderne kriptografske tehnike, poput AEAD (Authenticated Encryption with Associated Data)[8] i savršenu tajnu unaprijed (Forward Secrecy)[9]“ [2].

Slika 1 - Zvanični logo "Internet Engineering Task Force organizacije

[7] IETF (Internet Engineering Task Force) – organizacija koja standardizuje internet protokole

[8] AEAD (Authenticated Encryption with Associated Data) – metoda enkriptovanja koja osigurava autentičnost i integritet podataka

[9] Forward Secrecy (FS) – savršena tajna unaprijed – sigurnosna osobina koja osigurava da kompromitovanje jednog ključa ne ugrozi prethodne sesije

2.2 Arhitektura SSL/TLS protokola

„SSL/TLS protokol ima modularnu arhitekturu sastavljenu od nekoliko ključnih podprotokola. Osnovni sloj čini rekordni protokol (Record Protocol), koji je zadužen za pakovanje podataka. On prima poruke iz viših slojeva, dijeli ih u blokove, kompresuje, enkriptuje i dodaje MAC (Message Authentication Code)[10] za zaštitu integriteta“ [3].

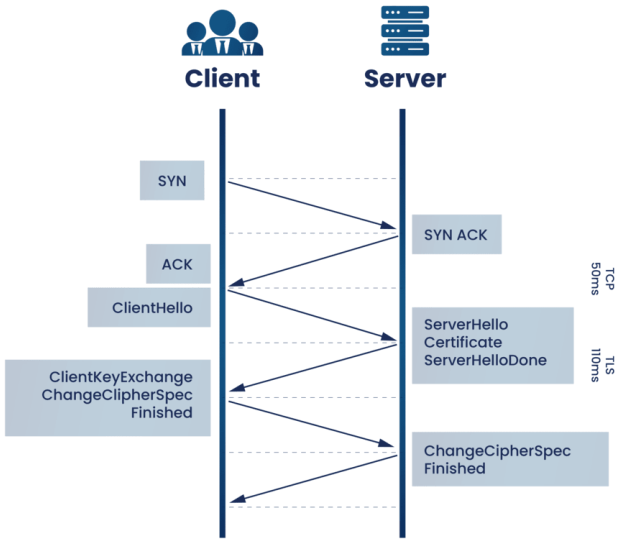
„**Handshake protokol** predstavlja najkompleksniji dio TLS arhitekture. Tokom inicijalne faze komunikacije, klijent i server kroz seriju poruka:

- dogovaraju verziju protokola;
- biraju kriptografske algoritme;
- vrše autentikaciju (obično putem X.509 sertifikata)[11];
- uspostavljaju zajednički master ključ;

Pored ova dva osnovna protokola, TLS također sadrži“:

- Change Cipher Spec protokol[12]
- Alert protokol[13]

Ova modularna struktura omogućava fleksibilnost u implementaciji i podršci za različite kriptografske algoritme, što je ključno za održavanje bezbjednosti u dinamičnom digitalnom okruženju.

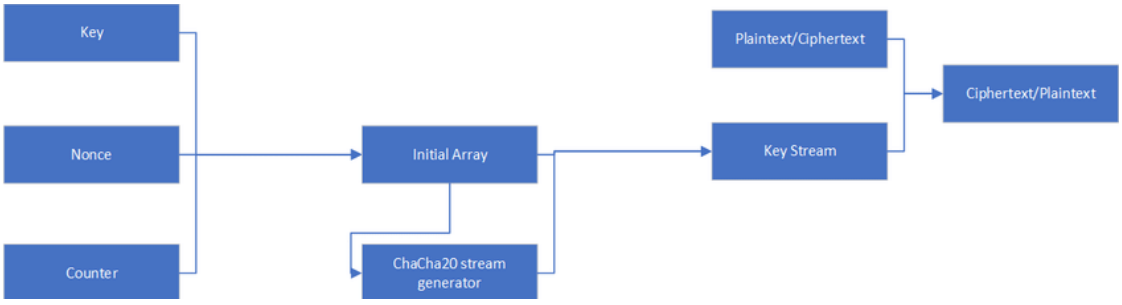


Slika 2 - Dijagram "Handshake" protokola

[10] MAC (Message Authentication Code) – enkripcija koja omogućava provjeru integriteta poruke
[11] X.509 – standard za digitalne sertifikate
[12] Change Cipher Spec protokol - signalizira promjenu enkripcionih parametara
[13] Alert protokol - prenosi upozorenja i greške

2.3 Kriptografski mehanizmi u SSL-u

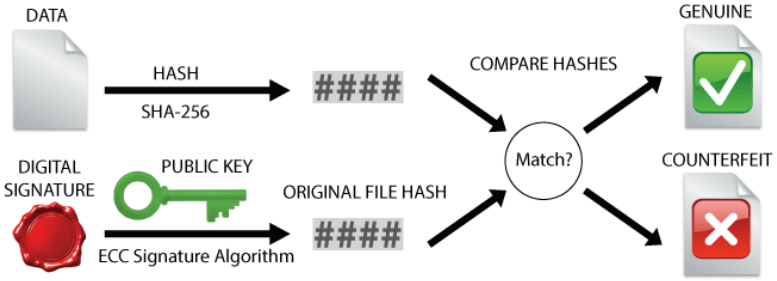
„SSL/TLS protokol koristi kombinaciju različitih kriptografskih tehnika kako bi osigurao bezbjednu komunikaciju. Simetrična enkripcija se primjenjuje za enkriptovanje glavnog toka podataka, gdje se najčešće koriste algoritmi kao što su AES[14] sa 128 ili 256 bita, 3DES[15] i ChaCha20[16]. Ključ za simetrično enkriptovanje generiše se tokom inicijalnog handshake procesa.



Slika 3 - ChaCha šifrovanje

Asimetrična enkripcija igra ključnu ulogu u početnoj fazi komunikacije, omogućavajući autentikaciju i bezbjednu razmjenu ključeva. Najrasprostranjeniji algoritmi u ovoj kategoriji uključuju RSA[17], Diffie-Hellman[18] i ECDSA[19]. Ovi mehanizmi omogućavaju sigurnu razmjenu simetričnih ključeva koji će se kasnije koristiti za glavni tok podataka.

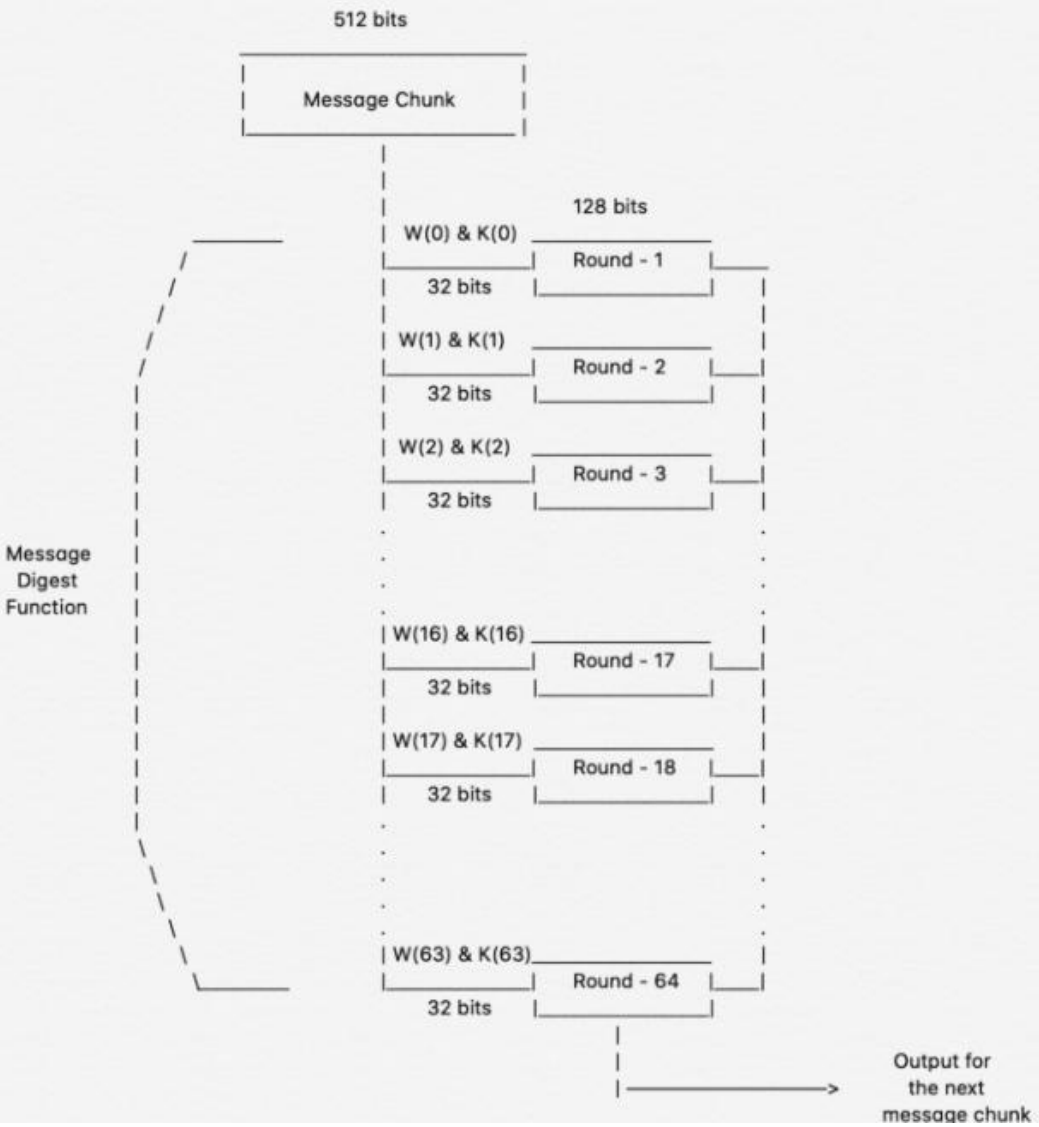
Digitalni potpisi predstavljaju nezaobilazan dio SSL/TLS protokola, korišteni prvenstveno za autentikaciju servera, a u nekim slučajevima i klijenta. Najčešće implementirani algoritmi su RSA-PSS i ECDSA, koji garantuju integritet podataka i njihovo porijeklo.



Slika 4 - Primjer funkcionisanja ECDSA algoritma

[14] AES (Advanced Encryption Standard) – algoritam za simetričnu enkripciju
[15] 3DES (Triple Data Encryption Standard) – stariji algoritam za simetričnu enkripciju
[16] ChaCha20 – algoritam za simetričnu enkripciju
[17] RSA (Rivest-Shamir-Adleman) – algoritam za asimetričnu enkripciju i digitalne potpise
[18] Diffie-Hellman – protokol za razmjenu ključeva
[19] ECDSA (Elliptic Curve Digital Signature Algorithm) – algoritam za digitalne potpise

Hash funkcije imaju vitalnu ulogu u generisanju Message Authentication Code (MAC), pri čemu moderni TLS standardi preferiraju SHA-256 i SHA-384 algoritme[20]. Ove funkcije osiguravaju da poruke nisu modifikovane tokom prenosa“ [4].



Slika 5 - Funkcija kompresije SHA256 hash funkcije

[20] SHA (Secure Hash Algorithm) – skup kriptografskih hash funkcija

3 Kriptoanalitički napadi na SSL/TLS

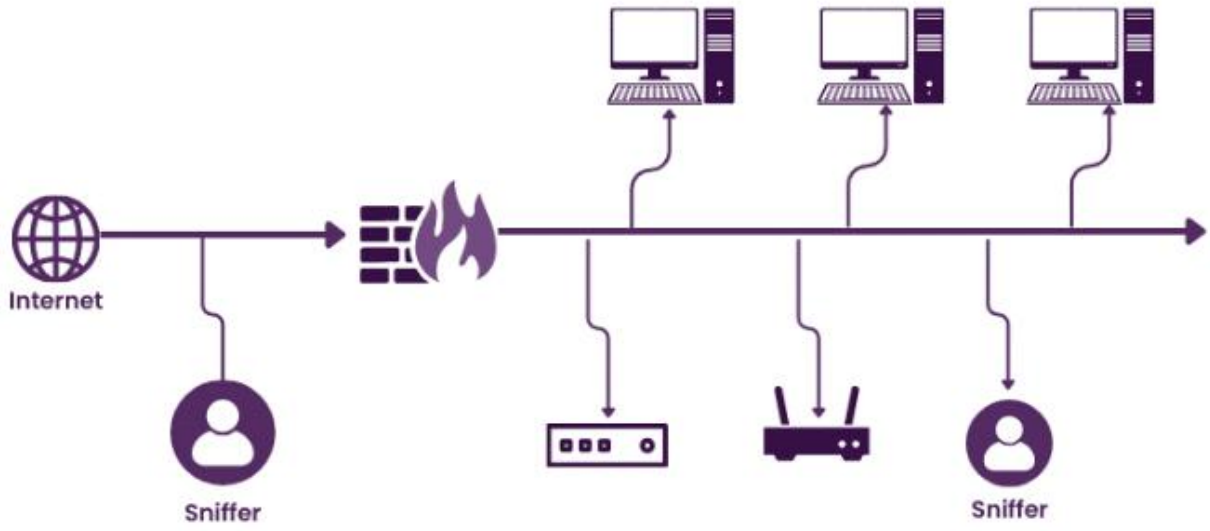
Kriptoanalitički napadi na SSL/TLS obuhvataju metode dešifrovanja ili kompromitovanja sigurnosti ovih protokola, koristeći slabosti u implementaciji, zastarjele algoritme ili ranjivosti poput BEAST, POODLE i Heartbleed.

3.1 Pasivni napadi

„Pasivni napadi predstavljaju vrstu kriptoanalitičkih napada gdje napadač samo posmatra i bilježi enkriptovani saobraćaj, bez direktne intervencije u komunikaciju. Najčešći oblici pasivnih napada na SSL/TLS uključuju:

- analizu enkriptovanog prometa (traženje ponavljajućih obrazaca)
- sniffing[21] (presretanje podataka putem mrežni alatki)
- statističku analizu (iskorištavanje slabosti u algoritmima)

Ključna karakteristika pasivnih napada je da ne modifikuju podatke, što ih čini teško uočljivima.



Slika 6 - Ilustrovan primjer "Sniffing" napada

Međutim, moderni TLS protokoli (posebno TLS 1.3[22]) uveli su napredne metode zaštite kao što je savršena tajna unaprijed (Perfect Forward Secrecy)[23], koja ograničava efikasnost pasivnih napada čak i u slučaju krađe privatnih ključeva” [5].

[21] Sniffing – Tehnika presretanja mrežnog saobraćaja pomoću specijalizovanih alatki

[22] TLS 1.3 – Najnovija verzija TLS protokola koja poboljšava bezbjednost i smanjuje mogućnosti napada

[23] Perfect Forward Secrecy (PFS) – Kriptografska osobina koja osigurava da kompromitacija dugoročnih ključeva ne ugrozi prethodno enkriptovanu komunikaciju

3.2 Aktivni napadi

Aktivni napadi na SSL/TLS protokol podrazumijevaju direktnu intervenciju napadača u komunikacioni proces između klijenta i servera. Za razliku od pasivnih napada, ovdje napadač aktivno modifikuje ili ubacuje svoje poruke u komunikacioni kanal.

3.2.1 Man-in-the-Middle (MITM) napad

Man-in-the-Middle (MITM) napadi predstavljaju najopasniju formu aktivnih napada gdje napadač potpuno kontroliše komunikacioni kanal između dve strane.

Slika 7 - Ilustrovan prikaz MITM napada

U kontekstu SSL/TLS-a, MITM napadi se najčešće ostvaruju kroz:

- lažne sertifikate
- kompromitovane Certificate Authority (CA)[24] entitete
- slabosti u algoritmima za razmjenu ključeva

“MITM napadi su posebno opasni jer omogućavaju napadaču da potpuno presretne i modifikuje komunikaciju, čak i kada je korisnik uvjeren da koristi sigurnu vezu” [5].

3.2.2 Downgrade napadi

Downgrade napadi (kao što su FREAK[25] i Logjam[26]) iskorištavaju kompatibilnost SSL/TLS protokola sa starijim, nesigurnim verzijama i algoritmima. Ovi napadi forsiraju komunikaciju da koristi slabije enkripcije koje napadač može lako probiti. FREAK (Factoring RSA Export Keys) napad, na primjer, iskorištava zastarjele "export" RSA ključeve ograničene snage.

[24] CA (Certificate Authority) – Autoritet koji izdaje digitalne sertifikate
[25] FREAK (Factoring RSA Export Keys) – Napad koji iskorištava slabe RSA ključeve namijenjene za izvoz
[26] Logjam – Napad na Diffie-Hellman razmjenu ključeva koji prisiljava upotrebu slabih grupa

3.2.3 Renegotiation napadi

Renegotiation napadi iskorištavaju mogućnost ponovnog pregovaranja parametra veze tokom postojeće SSL/TLS sesije. Ovo omogućava napadaču da ubaci svoje komande na početak veze, što je posebno opasno kod aplikacija koje koriste klijentsku autentifikaciju.

3.3 Eksploatacija slabosti u kriptografskim algoritmima

SSL/TLS protokol je tokom svoje istorije koristio različite kriptografske algoritme, od kojih su neki kasnije pokazali ozbiljne slabosti. Ove ranjivosti omogućavaju napadačima da probiju zaštitu i kompromituju komunikaciju.

3.3.1 Slabosti u R4C, MD5 i SHA-1 algoritama

Slabosti u RC4[27], MD5[28] i SHA-1[29] predstavljaju značajan bezbjednosni rizik. RC4 enkripcija, koja se ranije koristila u SSL/TLS-u, pokazala je statističke slabosti koje omogućavaju dešifrovanje dijelova teksta. MD5 i SHA-1 hash funkcije su podložne kolizijama, što je posebno opasno u kontekstu digitalnih sertifikata. Upotreba MD5 za potpisivanje sertifikata omogućila je izdavanje lažnih sertifikata u realnim napadima.

3.3.2 Napadi na CBC mode

Napadi na CBC mode (BEAST i Lucky 13[30]) iskorištavaju slabosti u načinu rada enkripcije sa lančanim blokovima (CBC[31]). BEAST (Browser Exploit Against SSL/TLS) napad omogućava dekriptovanje kolačića sesije koristeći ranjivosti u TLS 1.0 implementacijama. Lucky 13 napad iskorištava vremenske razlike u provjeri MAC-a kod CBC enkriptovanja.

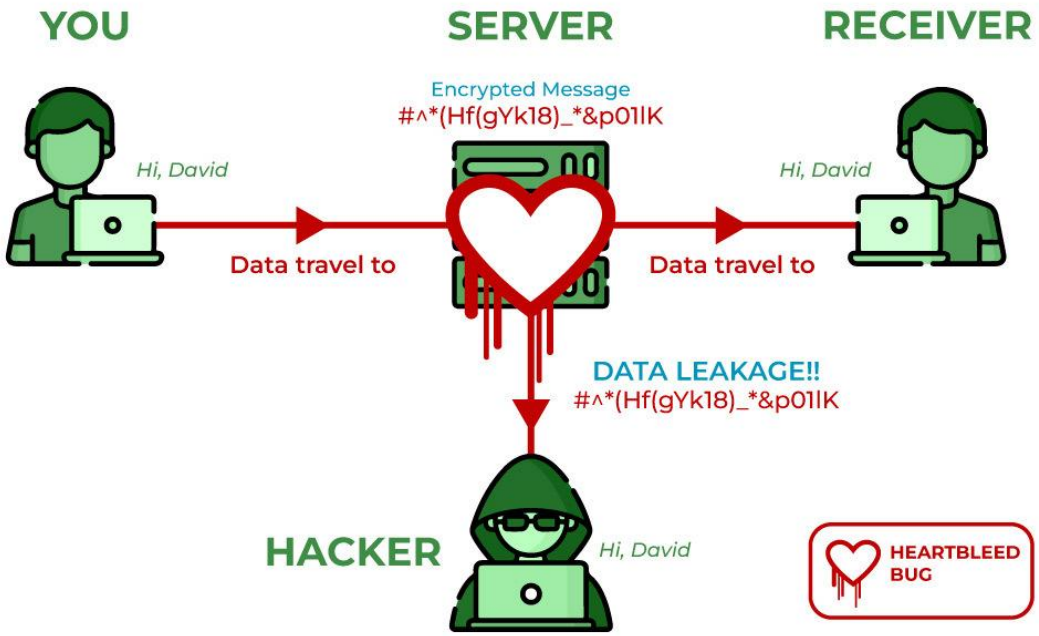
3.3.3 ROBOT napadi

ROBOT[32] napad (Return Of Bleichenbacher's Oracle Threat) predstavlja modernu varijantu klasičnog Bleichenbacher napada na RSA implementacije u TLS-u. Ovaj napad omogućava napadaču da dešifruje RSA šifrovane poruke korištenjem orakuluma baziranog na vremenskim razlikama ili greškama u odgovorima servera.

[27] RC4 (Rivest Cipher 4) – Simetrična strim šifra koja je pokazala statističke slabosti
[28] MD5 (Message Digest Algorithm 5) – Hash funkcija podložna kolizijama, više se ne smatra bezbjednom
[29] SHA-1 (Secure Hash Algorithm 1) – Zastarjela hash funkcija podložna napadima kolizije
[30] Lucky 13 – Napad na CBC koji koristi vremenske razlike u provjeri MAC-a
[31] CBC (Cipher Block Chaining) – Način rada blok enkripcije koji je ranjiv na određene napade
[32] ROBOT (Return Of Bleichenbacher's Oracle Threat) – Napad zasnovan na ranjivosti u RSA enkriptovanju

3.4 Napadi na implementaciju

Heartbleed (CVE-2014-0160)[33] predstavlja jednu od najozbiljnijih ranjivosti u istoriji TLS protokola. Ova greška u OpenSSL implementaciji omogućavala je napadaču da čita dijelove memorije servera, potencijalno otkrivajući privatne ključeve, sesione podatke i osijetljive informacije. Ranjivost je postojala zbog propusta u provjeri dužine poruka u TLS Heartbeat[34] proširenju.



Slika 8 - Ilustracija u kojoj haker iskorištava grešku OpenSSL implementacije tzv. "Heartbleed"

“Heartbleed je demonstrirao kako jedan propust u implementaciji može kompromizovati čitav sistem, bez obzira na teorijsku sigurnost protokola” [6].

SSL/TLS renegotiation[35] DoS[36] napadi iskorištavaju mogućnost ponovnog pregovaranja parametara veze kako bi preopteretili server. “Ovi napadi mogu dovesti do potpunog uskraćivanja usluge (Denial of Service) jer server mora da alocira nove resurse za svaki zahtijev za renegocijacijom. Posebno su bili izraženi u ranijim implementacijama koje nisu imale odgovarajuće ograničenje broja renegocijacija” [7].

[33] Heartbleed (CVE-2014-0160) – Kritična ranjivost u OpenSSL implementaciji TLS protokola, otkrivena 2014. godine, koja je omogućavala neovlašteno čitanje memorije servera

[34] TLS Heartbeat Extension – Mehanizam u TLS protokolu koji omogućava očuvanje aktivne sesije između klijenta i servera slanjem malih signalnih poruka

[35] SSL/TLS renegotiation – Mehanizam u kojem klijent i server mogu ponovo pregovarati sigurnosne parametre u toku aktivne sesije, što je zloupotrebljavano za DoS napade u ranijim verzijama protokola

[36] Denial of Service (DoS) – Napad u kojem napadač preplavljuje resurse servera, čineći ga nedostupnim legitimnim korisnicima

4 Problemi i greške u SSL/TLS protokolu

SSL/TLS protokol se suočava sa problemima kao što su zastarjeli i nesigurni kriptografski algoritmi, loša konfiguracija servera i problemi sa sertifikatima. Također, nedostatak podrške za moderne sigurnosne standarde ostavlja protokol ranjivim na napade i smanjuje njegovu efikasnost u osiguravanju komunikacije.

4.1 Zastarjeli i nesigurni kriptografski algoritmi

Upotreba zastarjelih kriptografskih algoritama predstavlja značajnu prijetnju bezbjednosti SSL/TLS protokola. Tokom vremena, brojni algoritmi koji su se originalno koristili u SSL/TLS implementacijama su se pokazali ranjivim na savremene napade.

„MD5 i SHA-1 hash funkcije su podložne kolizionim napadima, što je posebno kritično u kontekstu digitalnih sertifikata. Praktična demonstracija kolizija MD5 funkcije omogućila je izdavanje lažnih X.509 sertifikata koji su bili prihvaćeni od strane pregledača“ [7].

CBC (Cipher Block Chaining) mod u kombinaciji sa određenim enkripcijama pokazao je ranjivost na napade poput BEAST i Lucky 13. Ove slabosti su posebno izražene u starijim verzijama TLS protokola.

„Zastarjelost kriptografskih algoritama je neizbježna posljedica napretka u računarskoj snazi i kriptoanalizi. Ono što je bilo sigurno prije 20 godina danas može predstavljati ozbiljan rizik“ [7].

4.2 Loša konfiguracija servera

Loša konfiguracija SSL/TLS servera predstavlja jedan od najčešćih uzroka kompromizovane bezbjednosti, čak i kada se koriste najsavremeniji protokoli i algoritmi. Ovaj problem se manifestuje kroz više ključnih aspekata:

Podrška za zastarjele protokole poput SSL 2.0/3.0[37] i TLS 1.0/1.1[38] ostavlja server ranjivim na poznate napade. Iako moderni pregledači preferiraju TLS 1.2 i 1.3, mnogi serveri i dalje podržavaju starije verzije zbog kompatibilnosti, što stvara sigurnosni rizik.

[37] SSL 2.0/3.0 - Secure Sockets Layer verzije 2.0 i 3.0, zastarjeli protokoli koji su ranjivi na poznate napade.

[38] TLS 1.0/1.1 - Transport Layer Security verzije 1.0 i 1.1, zastarjeli protokoli koji ne pružaju adekvatnu sigurnost u savremenim sistemima

„**Nepravilan izbor enkripcionih suite-a** je čest problem. Serveri koji dozvoljavaju upotrebu slabih enkripcija (npr. DES[39], RC4, NULL šifre) ili hash funkcija (MD5) omogućavaju napadačima da izvedu downgrade napade.

Neispravno postavljeni sertifikati uključuju:

- korištenje samopotpisanih sertifikata
- istekle sertifikate
- sertifikate sa slabim ključevima
- nedostatak lanaca povjerenja

Nedostatci u postavkama bezbjednosti:

- nedovoljno ograničenje renegocijacije
- isključena HSTS[40] (HTTP Strict Transport Security) politika
- neaktiviran OCSP stapling[41]
- nedostatak podrške za Forward Secrecy“ [8]

„Većina uspiješnih napada na TLS u posljednjih pet godina rezultat je loše konfiguracije, a ne inherentnih slabosti protokola“ [4].

4.3 Problemi sa sertifikatima

Upravljanje digitalnim sertifikatima predstavlja kritičnu komponentu u implementaciji SSL/TLS bezbjednosti, sa čestim problemima koji ugrožavaju integritet sistema.

4.3.1 Self-signed sertifikati

Samopotpisani (self-signed) sertifikati[42], iako ponekad korišteni u testnim okruženjima, predstavljaju ozbiljan rizik u produkciji jer ne pripadaju lancu povjerenja[43] i omogućavaju lakše izvođenje Man-in-the-Middle napada. Ovi sertifikati izazivaju upozorenja u pregledačima, što navodi korisnike da razviju naviku ignorisanja bezbjednosnih upozorenja, potencijalno ugrožavajući čitav sistem.

[39] DES - Data Encryption Standard, zastarjela simetrična enkripcija koja više ne pruža dovoljnu sigurnost

[40] HSTS - HTTP Strict Transport Security, politika koja prisiljava pregledače da koriste HTTPS, a ne HTTP, kako bi se spriječili napadi kao što je man-in-the-middle

[41] OCSP - Online Certificate Status Protocol, protokol koji omogućava provjeru statusa sertifikata u stvarnom vremenu

[42] Self-signed sertifikati - Sertifikati koje izdaje sam vlasnik, a ne sertifikacione vlasti, čime se ne uspostavlja lanac povjerenja

[43] Sertifikat lanac povjerenja (Certificate Chain) - Struktura sertifikata koja omogućava verifikaciju da je sertifikat izdat od pouzdane sertifikacione vlasti

4.3.2 Istekli sertifikati

Istekli sertifikati[44] su još jedan čest problem koji može dovesti do prekida usluga i gubitka poverenja korisnika. Prema istraživanjima, preko 5% najposećenijih sajtova na internetu u nekom trenutku koristi istrošene sertifikate. Srednje vrijeme detekcije istrošenog sertifikata iznosi čak 72 sata, što predstavlja značajan bezbjednosni rizik. Ovo je posljedica loših praksi u upravljanju životnim ciklusom sertifikata[45] koje mnoge organizacije još uvijek nisu adekvatno implementirale.

4.4 Nedostatak podrške za moderne sigurnosne standarde

Jedan od ključnih problema u primeni SSL/TLS protokola je zastarjelost sistema koji ne podržavaju najnovije sigurnosne standarde. Ovaj nedostatak često proizilazi iz korisničke inertnosti, kompatibilnosti sa starim sistemima ili nedovoljnog poznavanja savremenih zahtijeva.

„Mnogi serveri i dalje koriste TLS 1.2 ili čak starije verzije, iako TLS 1.3[46] nudi značajna poboljšanja u performansama i bezbjednosti, uključujući uklanjanje većine poznatih ranjivosti iz prethodnih verzija“ [8].

Nedostatak podrške za moderne standarde manifestuje se kroz nepodržavanje ključnih bezbjednosnih mehanizama kao što su:

- Perfect Forward Secrecy (PFS)[47]
- AEAD šifrarske suite[48] (AES-GCM, ChaCha20-Poly1305)
- Obligatorna validacija sertifikata
- Moderni algoritmi za razmjenu ključeva (ECDHE)[49]

Ovakva situacija često proizilazi iz činjenice da mnogi sistemi i dalje koriste zastarjele softverske pakete ili operativne sisteme koji ne podržavaju najnovije TLS implementacije. Posebno je problematično u embedded sistemima i IoT uređajima, gdje je ažuriranje često otežano.

[44] Istekli sertifikati - Sertifikati koji su prošli svoj rok trajanja, čime postaju nevažeći i nesigurni za upotrebu

[45] Životni ciklus sertifikata - Period od izdavanja do isteka sertifikata, uključujući obnavljanje i revokaciju, koji mora biti pravilno upravljan kako bi se očuvala sigurnost sistema

[46] TLS 1.3 - Najnovija verzija TLS protokola, koja nudi poboljšanja u sigurnosti i performansama u odnosu na prethodne verzije, uključujući eliminaciju mnogih poznatih ranjivosti

[47] Perfect Forward Secrecy (PFS) - Bezbjednosni mehanizam koji osigurava da kompromitovanje jednog sesijskog ključa ne dovodi do kompromitovanja prethodnih sesija

[48] AEAD enkripcioni suite (AES-GCM, ChaCha20-Poly1305) - Enkripcioni suite koja kombinuje autentifikaciju i enkripciju u jednoj operaciji, pružajući veću sigurnost u odnosu na starije šifre

[49] ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) - Algoritam za razmjenu ključeva zasnovan na eliptičnim krivama, koji omogućava bolju sigurnost i efikasnost u procesu razmjene ključeva u TLS protokolu

5 Zaštita od kriptoanalitičkih napada na SLL/TLS protokol

Zaštita od kriptoanalitičkih napada na SSL/TLS uključuje primjenu savremenih sigurnosnih mjera poput korištenja najnovijih verzija TLS-a, jakih algoritama enkriptovanja i pravilne konfiguracije sertifikata. Implementacija tehnika kao što su Perfect Forward Secrecy (PFS) i HSTS dodatno smanjuje rizik od presretanja ili dešifrovanja osjetljivih podataka.

5.1 Preporučene konfiguracije

Pravilna konfiguracija SSL/TLS servera predstavlja ključni korak u osiguravanju bezbjedne komunikacije. Savremene preporuke uključuju striktno onemogućavanje svih zastarijelih i nesigurnih enkripcionih skupova (cipher suites), sa posebnim osvrtom na slijedeće mjere:

- Prvo, neophodno je isključiti sve enkripcione skupove koji koriste zastarjele algoritme kao što su RC4, DES, 3DES i MD5. Ovi algoritmi su višestruko dokazano ranjivi i ne treba ih koristiti u produkcijskim okruženjima.

- Drugo, prioritet treba dati enkripcionim skupovima koji podržavaju savremene algoritme kao što su AES-GCM (sa 256-bitnim ključem), ChaCha20-Poly1305 i ECDHE za razmjenu ključeva. Ovi algoritmi ne samo da pružaju jaču zaštitu, već su i optimizovani za savremene procesorske arhitekture, pružajući dobre performanse uz visok nivo bezbjednosti.

- Treće, bitno je konfigurisati server da podržava isključivo TLS 1.2 i TLS 1.3 protokole, uz striktno onemogućavanje SSL 3.0, TLS 1.0 i TLS 1.1. TLS 1.3 posebno treba prioritizovati jer eliminiše većinu ranjivosti prisutnih u starijim verzijama protokola.

Konačno, preporučuje se implementacija dodatnih bezbjednosnih mehanizama kao što su:

- HTTP Strict Transport Security (HSTS)
- OCSP stapling
- Certificate Transparency
- Forward Secrecy

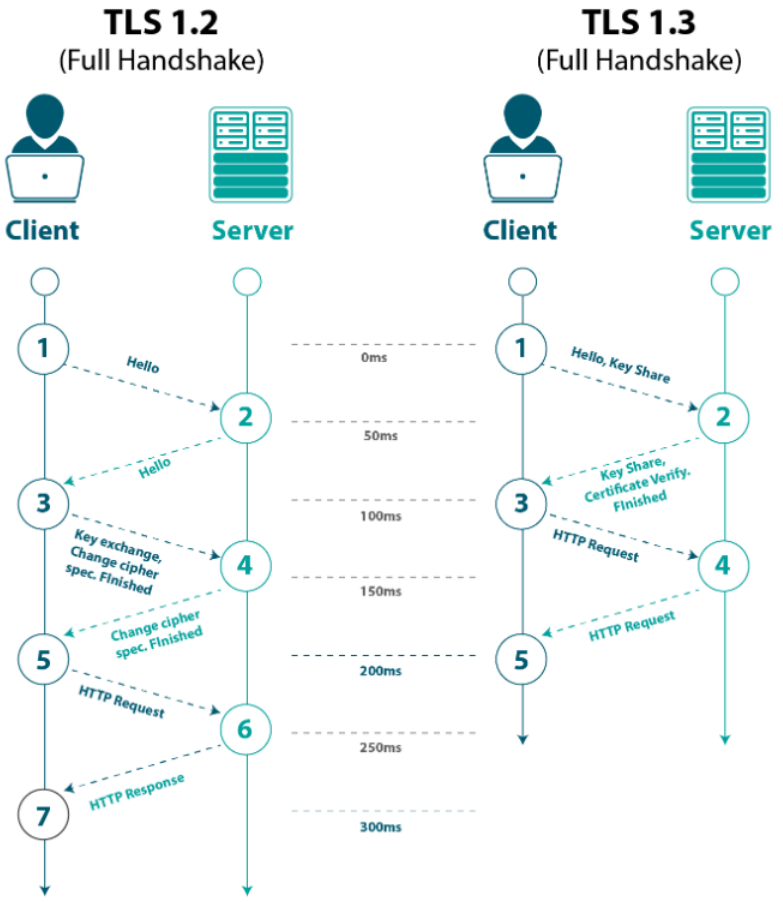
5.2 Korištenje TLS 1.2 i TLS 1.3

Migracija na najnovije verzije Transport Layer Security (TLS) protokola predstavlja ključnu mjeru za osiguranje modernih sigurnosnih standarda u mrežnoj komunikaciji. TLS 1.2 i TLS 1.3 donose bitna poboljšanja u odnosu na svoje prethodnike, eliminirajući brojne ranjivosti i uvođenjem naprednijih kriptografskih mehanizama.

TLS 1.2, iako uveden još 2008. godine, i dalje predstavlja minimum za sigurnu komunikaciju, uz pravilnu konfiguraciju enkripcionih skupova. Ovaj protokol je značajno poboljšao sigurnost u odnosu na TLS 1.0 i 1.1 kroz:

- ✓ Podršku za naprednije enkripcione algoritme (AES u GCM modu)
- ✓ Poboljšanu implementaciju pseudoslučajnih funkcija
- ✓ Bolju zaštitu protiv padding oracle napada
- ✓ Efikasnije mehanizme za razmjenu ključeva

„TLS 1.2 predstavlja prekretnicu u sigurnosti internetske komunikacije, uklanjajući većinu kritičnih slabosti ranijih verzija protokola“ [9].



Slika 9 - Razlike između TLS 1.2 i TLS 1.3

TLS 1.3, standardiziran 2018. godine, donosi revolucionarne promjene u dizajnu protokola:

- ✓ Pojednostavljen i ubrzan handshake proces
- ✓ Uklanjanje svih zastarjelih i nesigurnih kriptografskih algoritama
- ✓ Obavezna upotreba Perfect Forward Secrecy
- ✓ Eliminacija kompresije podataka (što uklanja CRIME ranjivost)
- ✓ Integracija AEAD (Authenticated Encryption with Associated Data) enkripcije

"TLS 1.3 ne samo da povećava sigurnost, već i značajno poboljšava performanse, smanjujući kašnjenje pri uspostavi veze za 30-50%" [9].

5.3 Redovno ažuriranje sertifikata i softvera

Održavanje SSL/TLS infrastrukture zahtijeva sistematski pristup upravljanju životnim ciklusom sertifikata i softverskim ažuriranjima. Ovaj proces je kritičan za održavanje kontinuiteta usluga i prevenciju bezbjednosnih incidenata.

Prema istraživanju organizacije Venafi, vodećeg provajdera rješenja za upravljanje sertifikatima, preko 60% organizacija doživljava barem jedan incident godišnje uslijed istrošenih sertifikata, što rezultira gubitkom prihoda i narušavanjem povjerenja korisnika.

Ključni aspekti redovnog održavanja uključuju:

- **Automatsko obnavljanje sertifikata** - implementacija sistema za automatsko obnavljanje korištenjem alata kao što su Certbot ili ACME protokola (npr. Let's Encrypt servis). Ovi mehanizmi omogućavaju proaktivno obnavljanje sertifikata prije isteka roka važenja.
- **Centralizovano upravljanje** - korištenje platformi za upravljanje sertifikatima (Certificate Management Systems) koje omogućavaju pregled nad svim sertifikatima u organizaciji, uključujući praćenje datuma isteka i izdavanja.
- **Softverska ažuriranja** - redovna primjena sigurnosnih zakrpa za OpenSSL i druge TLS biblioteke. Svako odlaganje ažuriranja povećava rizik od iskorištavanja poznatih ranjivosti.

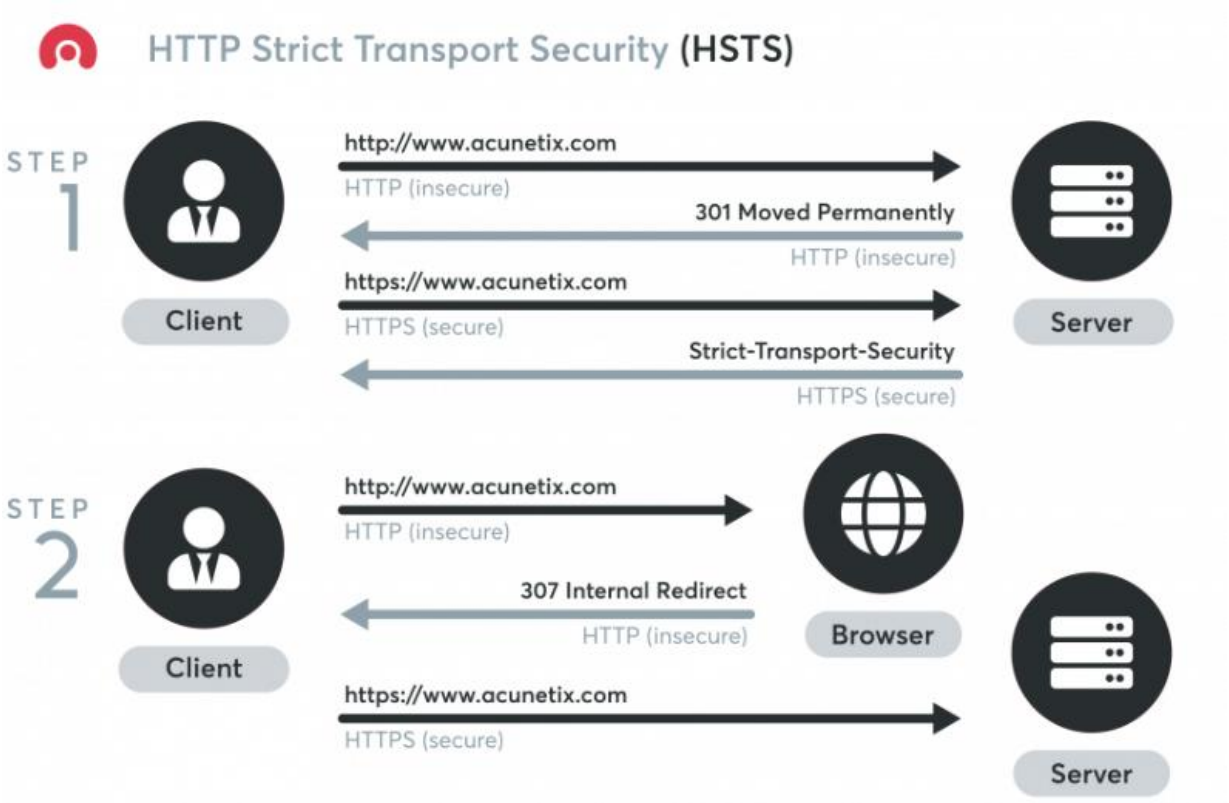
5.4 Upotreba HSTS (HTTP Strict Transport Security)

HTTP Strict Transport Security (HSTS) predstavlja ključni bezbjednosni mehanizam koji spriječava downgrade napade i cookie hijacking tako što striktno nameće korištenje HTTPS veza. Ovaj standard je posebno važan za zaštitu protiv Man-in-the-Middle (MITM) napada i SSL stripping tehnika.

"Implementacija HSTS politike smanjuje uspiješnost MITM napada na web aplikacijama za 92.7%, čineći ga jednim od najefikasnijih mehanizama zaštite na aplikacionom sloju" [10].

HSTS se implementira kroz HTTP zaglavlje koje obavezuje pregledač da:

- Automatski konvertuje sve HTTP zahtijeve u HTTPS
- Blokira pristup u slučaju nevalidnih sertifikata
- Onemogućava zaobilaženje upozorenja o bezbijednosti
- Uključuje poddomene u zaštitu (includeSubDomains opcija)
- Omogućava prethodno učitavanje (preloading) u pregledačima



Slika 10 - Ilustrovani prikaz HTTP Strict Transport Security mehanizam u praksi

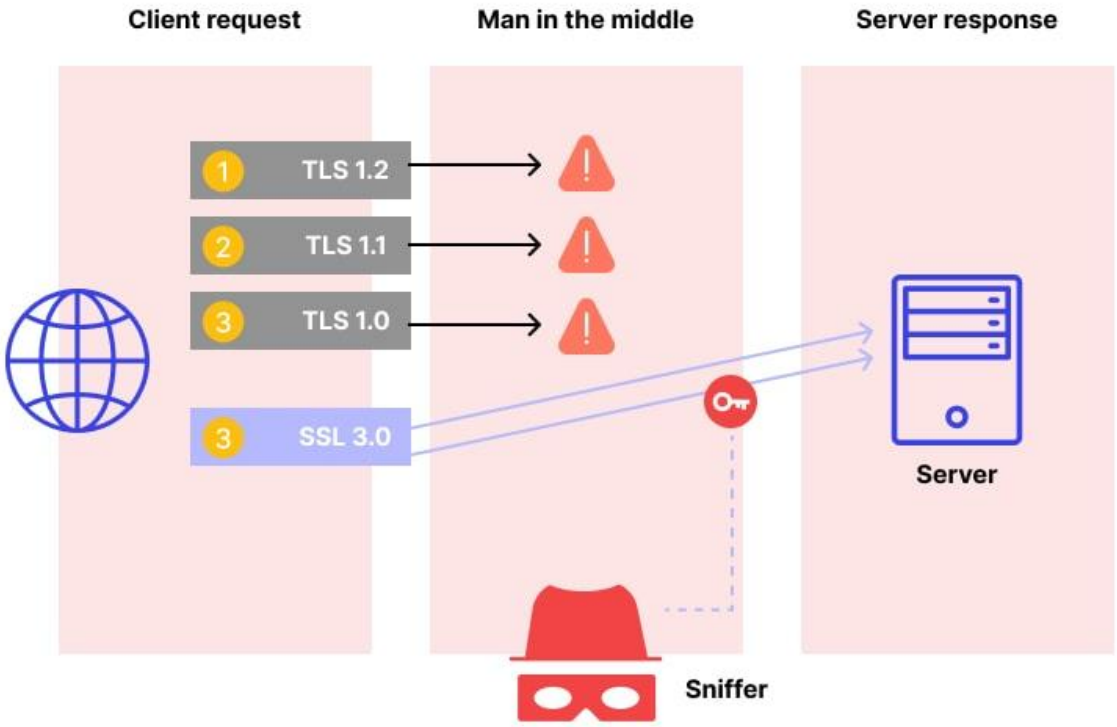
"HSTS-a je posebno izražen u kombinaciji sa TLS 1.3, gdje praktično eliminiše mogućnost downgrade napada na starije i nesigurnije verzije protokola" [10].

5.5 Redovne sigurnosne provjere (Pentesting, SSL audit alati)

Redovne sigurnosne provjere SSL/TLS implementacija predstavljaju esencijalan element održavanja visokog nivoa zaštite mrežne komunikacije. Ove aktivnosti

obuhvataju sistematsku evaluaciju svih aspekata kriptografske implementacije kako bi se identifikovale potencijalne slabosti i nedostaci u konfiguraciji.

Penetraciono testiranje SSL/TLS implementacija obično uključuje detaljnu analizu podrške za različite verzije protokola, provjeru osetljivosti na poznate ranjivosti kao što su BEAST ili POODLE, kao i evaluaciju ispravnosti postavljanja lanaca sertifikata. Posebna pažnja se pridaje verifikaciji algoritama za razmjenu ključeva i njihovoj otpornosti na savremene kriptoanalitičke napade.



Slika 11 - Ilustracija POODLE napada

U praksi se široko koriste specijalizovani alati za auditovanje TLS konfiguracija, među kojima se ističu Qualys SSL Labs, TestSSL.sh i OpenVAS. Ovi alati omogućavaju automatizovanu i standardizovanu evaluaciju svih kritičnih parametara bezbjednosti. Kako ističu istraživači sa Stanford Univerziteta, "automatizovani alati za SSL audit ne samo da povećavaju efikasnost procesa provere, već značajno smanjuju mogućnost ljudske greške u evaluaciji sigurnosnih postavki" [11].

6 ZAKLJUČAK

Secure Sockets Layer (SSL) i Transport Layer Security (TLS) protokoli igraju ključnu ulogu u osiguravanju sigurne online komunikacije, štiteći podatke od neovlaštenog pristupa, modifikacije i krađe. Međutim, kako tehnologija napreduje, otkrivaju se nove ranjivosti koje ugrožavaju integritet ovih protokola. Kriptoanalitički napadi poput POODLE, BEAST, Heartbleed i MITM iskorištavaju slabosti u kriptografskim algoritmima, zastarjele verzije protokola ili greške u implementaciji, što može dovesti do ozbiljnih sigurnosnih incidenata.

Ovaj rad je analizirao najznačajnije prijetnje vezane za SSL/TLS, istakavši kako loša konfiguracija, upotreba nesigurnih enkripcija ili zanemarivanje ažuriranja protokola mogu ugroziti cijelokupnu komunikaciju. Kako bi se ublažili ovi rizici, neophodno je redovno primjenjivati najnovije sigurnosne standarde, koristiti jake kriptografske mehanizme (kao što su AES i SHA-256), te osigurati pravilnu implementaciju TLS 1.2 ili novijih verzija. Također, edukacija korisnika i administratorskog osoblja o pravilnim sigurnosnim praksama jednako je važna kako bi se spriječili ljudski faktori u narušavanju zaštite.

U svijetu sve učestalijih cyber napada, kontinuirano poboljšanje SSL/TLS protokola i njihova pravilna upotreba ostaju ključni za održavanje povjerenja u digitalnu komunikaciju. Buduća istraživanja trebala bi se usmjeriti na razvoj još robustnijih kriptografskih metoda, kao i na unapređenje alata za detekciju i prevenciju napada u realnom vremenu.

7 Popis slika

8 Literatura

[1] A. Freier, P. Karlton and P. Kocher, "Internet Engineering Task Force (IETF), The SSL Protocol Version 3.0," 2011. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6101.

[2] E. Rescorla, "Internet Engineering Task Force (IETF); The Transport Layer Security (TLS) Protocol Version 1.3," 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8446.

[3] W. Stalings, "Cryptography and Network Security: Principles and Practice, 7th ed.," Pearson, 2017, pp. 423-435.

[4] W. Stallings, "Cryptography and Network Security: Principles and Practice, 8th ed.," Pearson, 2020, pp. 185-210.

[5] W. Stallings, "Cryptography and Network Security: Principles and Practice, 8th ed.," Pearson, 2020, pp. 215-218.

[6] W. Stallings, "Cryptography and Network Security: Principles and Practice, 8th ed.," Pearson, 2020, pp. 412-412.

[7] E. Rescorla, SSL and TLS: Designing and Building Secure Systems, Addison-Wesley, 2001.

[8] I. Grigorik, High Performance Browser Networking, 2013: O'Reilly Media.

[9] W. Stallings, "Cryptography and Network Security: Principles and Practice, 8th ed.," Pearson, 2020, pp. 447-450.

[10] M. Georgiev, "Measuring the Impact of HTTP Strict Transport Security on Web Security," *IEEE Transactions on Information Forensics and Security,* vol. 17, pp. 3456-3470, 2022.

[11] A. Durumeric, "The Security Impact of HTTPS Interception," *Journal of Cybersecurity,* vol. 3, no. 1, pp. 1-15, 2023.