Analiza sigurnosti domaćih veb sajtova

Ema Sinđelić

***Sadržaj* — Uprkos stalnoj borbi da se bezbednost i privatnost na polju elektronskog poslovanja održe na što većem nivou, porast sajber kriminala narušava poverenje i utiče na povećan broj zabrinutih korisnika. Uporedo sa usvajanjem novih tehnologija, neophodno je razvijati i metode zaštite od sajber kriminala kako bi korisnici usluga bili bezbedni. U ovom radu prikazaćemo negativne efekte primene savremenih tehnologija u elektronskom poslovanju, kao i na koji način se mogu prevazići upotrebom različitih tipova enkripcije i protokola. Takođe, prikazaćemo detaljan pregled analize sigurnosti veb sajtova bankarskih institucija u Srbiji kao i nekih poznatijih domaćih onlajn prodavnica.**

***Ključne reči* — elektronsko bankarstvo, elektronsko poslovanje, enkripcija, HTTPS, TLS.**

I. UVOD

Jedan od najvažnijih vidova poslovanja današnjice predstavlja elektronsko poslovanje koje se sve više razvija u bankarskom sektoru, što je doprinelo automatizaciji proizvoda i usluga banaka. Takođe, poslednjih par godina, sve više je prisutna onlajn kupovina putem koje su korisnici u prilici da kupuju najrazličitije proizvode bilo gde da se nalaze. Jedna od glavnih briga prilikom kupovine na mreži i pristupa finansijskim informacijama je sigurnost. Sigurnost informacija je zaštita informacija i sistema koji se koriste za čuvanje i prenos podataka. Kompanije se jako trude da osiguraju podatke svojih korisnika i steknu njihovo poverenje. Kako tehnologija nastavlja da

Ema Sinđelić, Računarski fakultet, Srbija (telefon: 381-64-1156160; e-mail: emasindjelic@gmail.com).

napreduje, mere bezbednosti se takođe poboljšavaju i postaju sve sofisticiranije.

U prvom delu rada biće objašnjeno na koji način se može postići sigurnost na transportnom sloju primenom SSL – *Secure Sockets Layer* ili TLS – *Transport Layer Security* protokola. Drugi deo rada odnosi se na sigurnosni aspekt HTTPS (*Hypertext Transfer Protocol Secure*) protokola. Na kraju rada prikazaćemo detaljan pregled analize sigurnosti veb sajtova domaćih banaka i onlajn prodavnica.

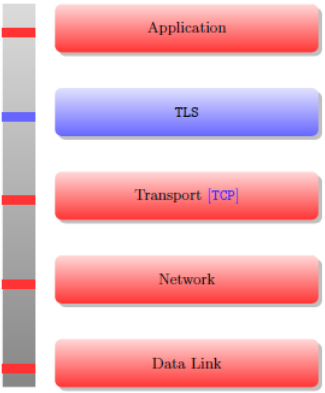
II. SIGURNOST NA TRANSPORTNOM SLOJU (TLS)

TLS, naslednik sada zastarelog SSL protokola, je kriptografski protokol dizajniran da obezbedi bezbednost komunikacije preko računarske mreže. Protokol se široko koristi u aplikacijama kao što su e-pošta, razmena poruka i glasa preko IP-a, ali njegova upotreba kao bezbednosnog sloja u HTTPS-u i dalje je najvidljivija.

TLS protokol ima za cilj prvenstveno da obezbedi privatnost i integritet podataka između dve ili više računarskih aplikacija koje komuniciraju. Pokreće se u aplikativnom sloju Interneta i sam se sastoji od dva sloja: TLS Record Protocol-a i TLS protokola rukovanja.

TLS je predloženi *Internet Engineering Task Force* (IETF) standard, prvi put definisan 1999. godine, a trenutna verzija je TLS 1.3 definisana u avgustu 2018. TLS se nadovezuje na ranije SSL specifikacije (1994., 1995., 1996.) koje je razvila *Netscape Communications* za dodavanje HTTPS protokola njihovom veb pregledaču *Navigator*.

TLS je mrežni protokol osmišljen za pružanje bezbednosnih usluga za protokole koji se izvode na aplikativnom sloju. TLS radi preko protokola transportnog sloja, kao što je prikazano na Sl. 1. Konkretno, TLS radi preko protokola za kontrolu prenosa TCP – *Transmission Control Protocol*, pouzdanog mrežnog protokola koji garantuje isporuku ispravnih mrežnih poruka. Primarni cilj TLS-a je da olakša uspostavljanje sigurnog kanala između dva komunikaciona entiteta, naime klijenta i servera.



Sl. 1. Konceptualno pozicioniranje TLS-a unutar TCP/IP modela arhitekture protokola. Mrežni slojevi su prikazani crvenom bojom. Mrežni protokoli su prikazani plavom bojom.

TLS protokol se sastoji od niza podprotokola, od kojih su dva najvažnija tzv. protokol rukovanja (*Handshake Protocol*) i *Record Protocol*. Protokol rukovanja pregovara o svim kriptografski relevantnim parametrima (uključujući TLS verziju, metodu autentifikacije i razmene ključeva i koji će se sledeći algoritmi simetričnih ključeva koristiti). On potvrđuje autentičnost jednog (ili oba) entiteta koji komuniciraju i uspostavlja ključeve za simetrične algoritme koji će se koristiti u *Record Protocol*-u za zaštitu aplikativnih podataka.

Na primer, ako se klijent i server dogovore da koriste TLS_RSA_SA_AES_128_CBC_SHA256 paket šifri tokom TLS 1.2 rukovanja, onda će server obezbediti RSA sertifikat koji će se koristiti za razmenu ključeva i autentifikaciju entiteta. U ovom primeru, *Record Protocol* će zatim koristiti *Advanced Encryption Standard* (AES) u *Cipher Block Chaining* (CBC) modu za šifrovanje podataka aplikacije, a heš funkcija SHA-256 će se koristiti u *Hash-based Message Authentication Code* (HMAC) algoritmu za obezbeđivanje autentifikacije poruka.

TLS takođe uključuje još jedan podprotokol, naime, Protokol upozorenja (*Alert Protocol*). Ovaj protokol se aktivira kada se jave greške u radu druga dva podprotokola. On će slati poruke upozorenja aplikativnom sloju, ukazujući na ozbiljnost upozorenja. Fatalna upozorenja će dovesti do trenutnog prekida TLS veze. Upozorenja su informativnog karaktera i ne moraju nužno dovesti do prekida veze.

TLS *Handshake Protocol* ima za cilj pregovaranje o kriptografskim ključevima putem mehanizma *Authenticated Key Exchange* (AKE). To znači da klijent i server ne samo da bezbedno uspostavljaju simetrične ključeve, već i da postoje garancije u vezi sa potraživanim identitetima strana koje komuniciraju. Ključevi uspostavljeni u protokolu rukovanja tada se koriste od strane *Record Protocol*-a za pružanje kritičnih bezbednosnih garancija, uključujući poverljivost i integritet aplikativnih podataka. TLS ima za cilj da obezbedi ove garancije u prisustvu aktivnog mrežnog napadača, tj. napadača koji može da uhvati, izmeni, izbriše, ponovo reprodukuje i na drugi način ometa poruke poslate preko komunikacionog kanala.

A. SSL protokol

SSL je protokol za sigurno slanje poruka (komuniciranje) putem Interneta, koji omogućuje slanje poverljivih podataka (npr. broj kreditne kartice) putem Interneta u šifrovanom i sigurnom obliku. SSL protokol ostvaruje poseban komunikacioni sloj, koji je smešten na pouzdan transportni sloj (npr. TCP/IP), dok se na SSL smešta aplikativni sloj. Od aplikativnog sloja prima poruku koju treba poslati, rastavi je u manje delove prikladne za šifrovanje, dodaje kontrolni broj, šifruje, eventualno kompresuje, a zatim te delove pošalje. Primalac primi delove, dekompresuje, dešifruje, proveri kontrolne brojeve, sastavi delove poruke, pa ih preda aplikativnom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mrežu. Ukoliko su klijent i server neaktivni duže vreme ili razgovor sa istim atributima zaštite potraje predugo, atributi se menjaju.

SSL omogućava razmenu informacija između klijenta i servera, na transparentan način. Ovaj protokol je lociran između aplikativnog i transportnog sloja ISO/OSI referentnog modela. Koristeći ovaj pristup, moguće je identifikovati SSL protokol kao deo sloja za prezentaciju. Međutim, SSL ne funkcioniše na vrhu *User Datagram protokola* (UDP), zato što ne nudi pouzdan prenos podataka, što može dovesti do gubitka IP paketa. Zbog toga, SSL ne može pružiti zaštitu za sledeće protokole: *Simple Network Management Protocol* (SNMP), *Network File System* (NFS), *Domain Name Service* (DNS), kao i za protokol „*voice over IP*“.

B. TLS 1.0, 1.1

TLS 1.0 je prvi put definisan u RFC 2246 u januaru 1999. kao nadogradnja SSL verzije 3.0, a napisali su ga Christopher Allen i Tim Dierks iz *Consensus Development*-a. Kao što je navedeno u RFC-u, „razlike između ovog protokola i SSL 3.0 nisu dramatične, ali su dovoljno značajne da isključe interoperabilnost između TLS 1.0 i SSL 3.0”.

Savet PCI je predložio da organizacije pređu sa TLS 1.0 na TLS 1.1 ili noviju pre 30. juna 2018. godine. U oktobru 2018. *Apple*, *Google*, *Microsoft* i *Mozilla* zajedno su najavili da će u martu 2020. ukinuti TLS 1.0 i 1.1.

TLS 1.1 je definisan u RFC 4346 u aprilu 2006. godine. To je ažuriranje sa TLS verzije 1.0. Značajne razlike u ovoj verziji uključuju:

- Dodatna zaštita od napada lančanog bloka šifara (CBC).
- Implicitni vektor inicijalizacije (IV) zamenjen je eksplicitnim IV.
- Promena u rukovanju greškama.
- Podrška za IANA registraciju parametara.

Podršku za TLS verzije 1.0 i 1.1 veb stranice su uveliko obustavile, onemogućavajući pristup verzijama *Firefox*-a pre 24. i *Google Chrome*-u pre 29. verzije.

C. TLS 1.2

TLS 1.2 je definisan u RFC 5246 u avgustu 2008. godine. Baziran je na specifikaciji prethodne verzije TLS 1.1. Glavne razlike uključuju:

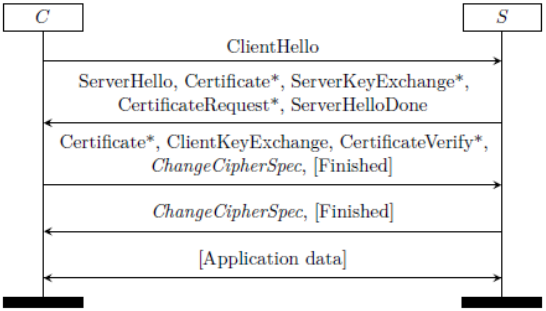
- Kombinacija heš algoritama MD5-SHA-1 zamenjena je sa SHA-256.
- Kombinacija MD5-SHA-1 zamenjena je sa SHA-256, sa opcijom korišćenja specifičnih heš algoritama. Međutim, veličina heša u gotovoj poruci mora i dalje biti najmanje 96 bita.
- Kombinacija MD5-SHA-1 u digitalnom potpisu zamenjena je jednim hešom dogovorenim tokom rukovanja, koji podrazumeva SHA-1.
- Poboljšanje sposobnosti klijenata i servera da odrede koje heš algoritme i algoritme digitalnog potpisa prihvataju.
- Proširenje podrške za autentifikovane algoritme šifrovanja, najviše za *Galois/Counter Mode* (GCM) i CCM režim šifrovanja.

U nastavku opisujemo strukturu TLS 1.2, pokrivajući različite načine rukovanja, *Record Protocol* i predviđene bezbednosne ciljeve i svojstva.

Protokol rukovanja

TLS 1.2 ima tri vrste rukovanja, uključujući inicijalno rukovanje za postavljanje TLS sesije, ponovno rukovanje radi ažuriranja kriptografskih parametara sesije i ponovno rukovanje za ponovljena rukovanja unutar sesije.

Inicijalno rukovanje. Tokovi poruka za početno rukovanje TLS 1.2 prikazani su na Sl. 2. Poruke označene zvezdicom su izborne ili zavise od situacije, a zagrade tipa „[. . .]" označavaju šifrovanje pomoću saobraćajnih ključeva aplikacije. Klijent i server razmenjuju poruke *ClientHello* i *ServerHello* radi dogovora o paketu šifri i razmene vrednosti za trenutnu upotrebu. Entiteti koji komuniciraju takođe razmenjuju kriptografske parametre (*ServerKeyExchange*, *ClientKeyExchange*) koji omogućavaju izvođenje *pre-master* tajne. Sertifikati i odgovarajuće verifikacione informacije (*Certificate*, *CertificateVerify*) šalju se za potrebe autentikacije entiteta. Glavna tajna se izvodi iz vrednosti dogovorene za tu upotrebu i *pre-master* tajne, a zatim se koristi za izvođenje aplikativnih saobraćajnih ključeva koje će koristiti *Record Protocol*. Završna poruka sadrži kod za proveru autentičnosti poruke (*Message Authentication Code* - MAC) tokom celog rukovanja, osiguravajući da klijent i server dele identičan prikaz rukovanja i da aktivni napadač nije promenio nijednu poruku rukovanja.



Sl. 2. TLS 1.2 početno rukovanje

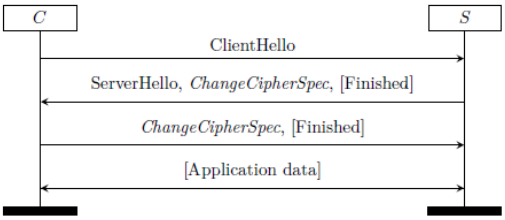
Protokol rukovanja radi preko *Record Protocol*-a, u početku sa nultom enkripcijom i MAC algoritmima. Poruke *ChangeCipherSpec* signaliziraju nameru da počnu koristiti nove kriptografske algoritme i ključeve; ove poruke se ne smatraju delom rukovanja, već su poruke ravnopravnog protokola, tj. protokola *ChangeCipherSpec* (protokol za promenu specifikacije šifrovanja). Pošto gotove poruke dolaze nakon poruka *ChangeCipherSpec*, one su zaštićene pomoću saobraćajnih ključeva aplikativnih podataka izvedenih u rukovanju. Ove poruke su, dakle, prve koje su zaštićene kao deo *Record Protocol*-a. Za njima slede poruke sa aplikativnim podacima, sada zaštićene *Record Protocol*-om.

TLS 1.2 omogućava statičku RSA razmenu ključeva, *Diffie-Hellman* razmenu ključeva, kao i kratkotrajnu *Diffie-Hellman* razmenu ključeva. U

slučaju RSA razmene ključeva, klijent će izabrati tajnu vrednost *pre-master*-a i šifrovati je sa javnim RSA ključem servera, primljenim u *Certificate* poruci servera. Ovo će formirati poruku klijenta *ClientKeyExchange*. U slučaju (kratkotrajne) *Diffie-Hellman* razmene ključeva, klijent i server će razmeniti *Diffie-Hellman* ključeve u porukama *ClientKeyExchange* i *ServerKeyExchange*, respektivno.

Ponovni pregovori (rukovanje). Kriptografski parametri uspostavljeni u početnom rukovanju čine TLS sesiju. Sesija se može ažurirati ponovnim rukovanjem. Ovo je potpuno rukovanje koje radi pod zaštitom već uspostavljene TLS sesije. Ovaj mehanizam omogućava promenu kriptografskih parametara (na primer, nadogradnju) ili zahtev servera za potvrdu identiteta klijenta (u slučaju da to prethodno nije zatraženo).

Nastavak sesije. Kako bi se izbegle skupe operacije sa javnim ključem u ponovljenim rukovanjima, TLS 1.2 takođe nudi lagano ponovno rukovanje u kojem se nova glavna tajna izvodi iz stare *pre-master* tajne i novih vrednosti za tu konkretnu upotrebu, čime se forsiraju novi ključevi aplikativnih podataka. Svako takvo ponovno rukovanje vodi do nove TLS veze unutar postojeće sesije; mnoge veze mogu postojati paralelno za svaku sesiju. Rukovanje za nastavak TLS 1.2 prikazano je na Sl. 3.



Sl. 3. TLS 1.2 ponovno rukovanje

Unapred deljeni ključevi (PSK-ovi, *Pre-Shared Keys*), u ovom slučaju simetrični ključevi uspostavljeni van opsega pre komunikacije, dozvoljeni su za upotrebu u TLS 1.2 u svrhe autentifikacije (važi i za niže verzije). Njihova upotreba je opisana u TLS ekstenzijama RFC 4279 i RFC 5487. Namera im je da izbegnu upotrebu skupih operacija sa javnim ključem.

Record Protocol pruža siguran kanal za prenos aplikativnih podataka (kao i protokol za rukovanje i protokol poruka upozorenja). U TLS 1.0 i 1.1, koristi konstrukciju *MAC-then-Encode-then-Encript* (MEE), pri čemu je MAC algoritam HMAC izveden sa nizom heš funkcija, a algoritam šifrovanja je izveden sa CBC načinom blok-šifre ili RC4 protočnom šifrom. Brojevi

sekvenci su uključeni u kriptografsku obradu, stvarajući zaštićen kanal sa statusom u kojem se mogu detektovati ponavljanja, brisanja i preuređivanja TLS zapisa. TLS 1.2 je dodao podršku za šeme autentifikovanog šifrovanja sa povezanim podacima (*Authenticated Encryption with Associated Data* - AEAD), i uz AES algoritam u Galoisovom načinu brojača (AES-GCM) ovo postaje sve popularnija opcija.

D. TLS 1.3

TLS 1.3. je definisan u RFC 8446. Baziran je na specifikaciji prethodne verzije TLS 1.2. Glavne razlike uključuju:

- Odvajanje razmene ključeva i algoritama za autentifikaciju.
- Uklanjanje podrške slabim i manje iskorišćenim eliptičnim krivama.
- Uklanjanje podrške za MD-5 i SHA-224 kriptografske heš funkcije.
- Zahtevanje digitalnih potpisa čak i kada se koristi prethodna konfiguracija.
- Integracija upotrebe sesijskog heša.
- Dodavanje protočnog algoritma ChaCha20 sa Poly1305 autentifikacijom.
- Dodavanje algoritama digitalnog potpisa Ed25519 i Ed 448.
- Dodavanje x25519 i x448 protokola za razmenu ključeva.

Zbog mnogih napada na TLS 1.2 i starije verzije, kao i zbog pritiska da se poboljša efikasnost protokola, IETF je od proleća 2014. radio na sledećoj verziji protokola, TLS 1.3. Polazeći u većoj meri od strukturnog oblika TLS 1.2, glavni ciljevi dizajna TLS 1.3 uključuju:

1. šifrovanje što je više moguće rukovanja,
2. ponovnu procenu sadržaja rukovanja,
3. smanjenje kašnjenja pri rukovanju - uvođenje *One Round-Trip Time* (1-RTT) za potpuna rukovanja i uvođenje *Zero Round-Trip Time* (0-RTT) za ponovljena rukovanja, i
4. ažuriranje mehanizama zaštite zapisa.

Šifrovanje rukovanja. Cilj koji teži poboljšanju enkripcije rukovanja jeste smanjenje količine vidljivih podataka kako pasivnim tako i aktivnim „neprijateljima“. Za razliku od TLS 1.2, koji komunikacionim entitetima

pruža samo ključeve sesije za zaštitu podataka aplikacije, TLS 1.3 predviđa uspostavljanje dodatnih ključeva sesije koji će se koristiti samo za svrhu enkripcije rukovanja. Šifrovanje rukovanja počinje odmah nakon što su ključevi za rukovanje pregovarani putem *Diffie-Hellman* razmene ključeva.

Sadržaj rukovanja. Struktura rukovanja je prepravljena radi efikasnosti. Dodatna poruka servera je uključena kako bi se prilagodilo slučaju neslaganja parametara, a kompresija aplikativnih podataka je uklonjena. Statički *Diffie-Hellman* i RSA uklonjeni su u korist savršene prosleđene tajne (*Perfect Forward Secrecy* - PFS) koja podržava kratkotrajni *Diffie-Hellman* (DHE) kao i kratkotrajni *Diffie-Hellman* uz kriptografiju eliptične krive (ECDHE). RSA sertifikati se i dalje koriste za autentifikaciju entiteta u DHE i ECDHE režimima. Potpisi na strani servera su obavezni u svim režimima rukovanja.

Trajanje rukovanja. Rukovanje TLS 1.2 zahtevalo je *Two Round-Trip Time* (2-RTT) pre nego što su komunikacioni entiteti mogli da prenesu aplikativne podatke. Rukovanje je preuređeno u TLS 1.3 tako da zahteva samo 1-RTT ako ne dođe do neslaganja parametara.

TLS 1.3 takođe uključuje opciju 0-RTT u kojoj je klijent u mogućnosti da šalje aplikativne podatke kao deo svoje prve iteracije poruka, nudeći jasnu prednost u efikasnosti u odnosu na TLS 1.2. Osim toga, već postojeći mehanizam za PSK proširen je na pokrivanje nastavka sesije. Ovaj režim takođe zahteva jedno kružno putovanje i manje iteracija od punog rukovanja.

Mehanizmi zaštite zapisa. Ranije verzije TLS-a koristile su generičku šemu sastava *MAC-then-Encript* kao mehanizam zaštite zapisa. Ova šema uopšte nije sigurna, i iako se i danas koristi u TLS 1.2, postojao je predlog da se ona zameni paradigmom *Encript-Then-MAC* (u RFC 7366). Slično, kada je Krawczyk najavio OPTLS protokol na TLS *mailing* listi, tj. protokol koji je trebao poslužiti kao teorijska osnova za TLS 1.3, izjavio je da će koristiti *Encript-then-MAC* za zaštitu zapisa. Konačno, radna grupa TLS odlučila je da će TLS 1.3 izbeći generičke šeme sastava i koristiti samo blok šifre koje mogu da rade u AEAD režimima. Stoga su sve šifre koje nisu AEAD uklonjene u TLS 1.3.

III. HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS)

Sigurni protokol za prenos hiperteksta (HTTPS) je proširenje protokola za prenos hiperteksta (HTTP). Koristi se za sigurnu komunikaciju preko računarske mreže, a široko se koristi i na Internetu. U HTTPS-u, komunikacioni protokol je šifrovan korišćenjem TLS-a ili, ranije, SSL

protokola. Protokol se stoga naziva i HTTP preko TLS-a, ili HTTP preko SSL-a.

HTTPS se često koristi u Internet bankarstvu jer se isti koristi za novčane transakcije i za prenos osetljivih informacija. Radi tako što koristi TLS mehanizme sa digitalnim sertifikatom koji koristi veb pretraživač. Sertifikati koje izdaju CA (*Certificate Authorities*) direktno se proveravaju od strane pretraživača. Tako, čak i sertifikati sa autoritetom mogu biti označeni kao validni ili nepoverljivi, ukoliko se primeti da ne ispunjavaju neke od uslova koje su CA propisale. Veb pretraživači onda znaju kako da veruju HTTPS veb stranicama na osnovu sertifikata koji dolaze preinstalirani na njihovom softveru.

Sigurnost HTTPS-a se ogleda u primeni osnovnog TLS-a, koji obično koristi dugotrajne javne i privatne ključeve za generisanje kratkoročnog ključa sesije, koji se zatim koristi za šifrovanje protoka podataka između klijenta i servera. X.509 sertifikati se koriste za autentifikaciju servera (a ponekad i klijenta). Zbog toga su ovlašćenja za izdavanje sertifikata i sertifikati javnih ključeva neophodni za proveru odnosa između sertifikata i njegovog vlasnika, kao i za generisanje, potpisivanje i administraciju valjanosti sertifikata.

Da bi HTTPS bio efikasan, veb sajt mora biti u potpunosti hostovan preko HTTPS-a. Ako je neki sadržaj veb sajta učitan preko HTTP-a (skripte ili slike, na primer), ili ako se samo određena stranica koja sadrži osetljive informacije, kao što je stranica za prijavljivanje, učitava preko HTTPS-a dok je ostatak veb sajta učitan preko običnog HTTP-a, korisnik će biti ranjiv na napade i nadzor. Osim toga, kolačići na veb sajtu koji se poslužuju putem HTTPS -a moraju imati omogućen bezbednosni atribut. Na veb sajtu koji sadrži osetljive informacije, korisnik i sesija će biti izloženi svaki put kada se tom veb sajtu pristupa sa HTTP umesto sa HTTPS.

Nedostaci HTTPS protokola. Sofisticirana vrsta napada „čovek-u-sredini“ pod nazivom *SSL stripping* predstavljena je na *Blackhat* konferenciji 2009. godine. Ova vrsta napada ugrožava bezbednost koju pruža HTTPS promenom *https:* linka u *http:* vezu, koristeći prednost činjenice da mali broj korisnika Interneta zapravo ukuca „*https*“ u interfejs svog pregledača: oni dolaze do bezbednog veb sajta klikom na vezu, pa se zavaravaju misleći da koriste HTTPS, a zapravo koriste HTTP. Napadač tada jasno komunicira sa klijentom. Ovo je podstaklo razvoj protivmere u HTTP-u pod nazivom *HTTP Strict Transport Security* (HSTS – omogućava veb sajtu da kaže pretraživačima da istom treba pristupiti samo pomoću HTTPS, umesto

pomoću HTTP; tokom analize koja sledi u narednom poglavlju prikazano je koji veb sajtovi podržavaju ovu funkcionalnost).

Pokazalo se da je HTTPS ranjiv na niz napada koji funkcionišu tako što se radi analiza saobraćaja. Napadi analize saobraćaja su vrsta bočnih kanala koji se oslanjaju na varijacije u vremenu i veličini saobraćaja kako bi se zaključilo o svojstvima samog šifrovanog prometa. Analiza saobraćaja je moguća jer SSL/TLS šifrovanje menja sadržaj saobraćaja, ali ima minimalan uticaj na veličinu i vremenski raspored saobraćaja. U maju 2010. godine, istraživački rad istraživača sa *Microsoft Research*-a i Univerziteta *Indiana* otkrio je da se detaljni osetljivi korisnički podaci mogu zaključiti iz sporednih kanala, poput veličine paketa. Istraživači su otkrili da bi, uprkos HTTPS zaštiti u nekoliko vrhunskih veb aplikacija u zdravstvu, oporezivanju, ulaganjima i pretraživanju veba, prisluškivač mogao zaključiti o bolestima/lekovima/operacijama korisnika, kao i o njegovom porodičnom prihodu i tajnim ulaganjima.

IV. Analiza sigurnosti odabranih veb sajtova

Za analizu sigurnosti veb sajtova odlučili smo se za alat koji je razvila kompanija *Qualys*. *Qualys, Inc. (NASDAK: KLIS)* je pionir i vodeći dobavljač rešenja za bezbednost i usklađenost zasnovanih na oblaku sa preko 9.300 kupaca u više od 100 zemalja. The *Qualys Cloud* platforma i integrisani paket rešenja pomažu organizacijama da pojednostave bezbednosne operacije i smanje troškove usklađenosti isporukom kritičnih bezbednosnih obaveštenja na zahtev i automatizacijom čitavog spektra revizije, usklađenosti i zaštite IT sistema i veb aplikacija. Osnovan 1999. godine, *Qualys* je uspostavio strateška partnerstva sa vodećim provajderima usluga i konsultantskim organizacijama, uključujući *Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro*. Kompanija je takođe jedan od osnivača *Cloud Security Alliance* (CSA).

Qualys-ov test SSL servera u suštini služi za skeniranje veb sajta radi utvrđivanja pogrešne konfiguracije kao i ranjivosti SSL/TLS-a. Omogućava detaljnu analizu https:// URL-a, uključujući dan isteka, ukupnu ocenu, šifre koje se koriste, SSL/TLS verziju, simulaciju rukovanja, detalje protokola i još mnogo toga.

U nastavku će biti prikazano nekoliko primera analiza veb sajtova domaćih banaka, od onih najboljih do onih slabije ocenjenih. Takođe, na kraju poglavlja biće prikazan pregled celokupne analize domaćih veb sajtova banaka i onlajn prodavnica koji su uzeti u obzir za ovaj rad.

A. Unicredit banka

Način autorizacije: korisničko ime i lozinka

Analiza sertifikata:

Izdavalac: Actalis Organization Validated Server CA G3

Ključ: RSA 2048 bits (e 65537)

Algoritam digitalnog potpisa: SHA256withRSA

Validan od 26.07.2021. do 26.07.2022.

Konfiguracija:

Protokol: Podržan protokol TLS verzije 1.2

Paket šifri:

- Server najviše preferira korišćenje dva potpuno sigurna paketa šifri, od kojih prvo paket šifri TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, a odmah zatim paket TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. Postoji i nekoliko WEAK paketa šifri, ali se ne koriste često, uglavnom kod pretraživača starijih verzija.

Detalji protokola:

Bezbedni ponovni pregovori: Podržani

POODLE napad: Ne, nije podržan SSL 3.0

RC4: Nije podržan

Forward Secrecy: Da, uglavnom sa svim pretraživačima

Ocena:

- Ukupna ocena je A+. Na ovako visoku ocenu uticala je podrška za protokol TLS 1.2 i to što su potpuno isključeni protokoli starijih verzija. Takođe, na ovom serveru razvijen je HSTS.

B. Halk banka

Način autorizacije: korisničko ime i lozinka

Analiza sertifikata:

Izdavalac: Go Daddy Secure Certificate Authority - G2

Ključ: RSA 2048 bits (e 65537)

Algoritam digitalnog potpisa: SHA256withRSA

Validan od 13.06.2020. do 16.06.2022.

Konfiguracija:

Protokol: Podržani su protokoli TLS 1.0, 1.1, 1.2 kao i 1.3

Paket šifri:

- Postoji više varijacija u zavisnosti od protokola koji se koristi. Prilikom simulacije rukovanja utvrđeno je da se najčešće koristi TLS 1.2, kao najčešći paket koristi se TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 koji je označen kao siguran. Što se tiče protokola TLS 1.3 najčešće se primenjuje paket TLS_AES_256_GCM_SHA384 takođe označen kao siguran. Naravno, obzirom da se i dalje koriste TLS 1.0 i 1.1, prilikom simulacije zabeleženo je korišćenje paketa TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA koji je manje siguran, a koristi se od strane *Android* pretraživača starijih verzija (ispod 4.3).

Detalji protokola:

Bezbedni ponovni pregovori: Podržani

Prevencija smanjenja napada: Da, TLS_FALLBACK_SCSV podržan

POODLE napad: Ne, ne podržava SSL 3.0

RC4: Ne podržava

Forward Secrecy: Da, sa uglavnom svih pretraživača

Ocena:

- Ukupna ocena je B. Na ocenu je uticalo to što se i dalje podržavaju starije verzije TLS-a 1.0 i 1.1, ali je takođe dosta doprinela podrška TLS verzije 1.3 što je veliki plus.

C. Poštanska štedionica

Način autorizacije: korisničko ime i lozinka

Analiza sertifikata:

Izdavalac: DigiCert Global G2 TLS RSA SHA256 2020 CA1

Ključ: RSA 2048 bits (e 65537)

Algoritam digitalnog potpisa: SHA256withRSA

Validan od 22.12.2020. do 22.01.2022.

Konfiguracija:

Protokol: Podržani su protokoli SSL 3.0, TLS 1.0, 1.1, 1.2

Paket šifri:

- Prilikom simulacije rukovanja najviše se koristi protokol TLS 1.2 verzije, a sam server nema preferenci kada koristi pakete šifri. Uglavnom je većina paketa označena kao WEAK odnosno manje sigurni paketi, postoje i oni potpuno nesigurni, npr. ovaj paket TLS_ECDHE_RSA_WITH_RC4_128_SHA ako se koristi sa SSL 3.0 protokolom izuzetno je nesiguran. Postoji i siguran paket TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 koji se koristi prilično često u toku simulacije.

Detalji protokola:

Bezbedni ponovni pregovori: Podržani

Prevencija smanjenja napada: Da, TLS_FALLBACK_SCSV podržan

POODLE napad: Ranjiv na ovaj napad, obzirom da podržava SSL 3.0

RC4: Podržava, ranjiv na RC4 napade

Forward Secrecy: Da, sa nekim pretraživačima

Ocena:

- Ukupna ocena je F. Na ovako negativnu ocenu uticala je podrška SSL 3.0 protokola koji je ranjiv na POODLE napade, takođe ovaj server je ranjiv na *OpenSSL Padding Oracle* ranjivost (CVE-2016-2107) i nije siguran (MITM napadač može koristiti *padding oracle* napad za dešifrovanje saobraćaja kada veza koristi AES CBC šifru, a ista se koristi uvidom u pakete šifri npr. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384), postoji podrška za RC4 protočnu šifru, podržava *Forward Secrecy* samo sa nekim pretraživačima, lanac sertifikata ovog servera nije potpun, kao i generalno podrška starijim verzijama TLS protokola 1.0 i 1.1 uticala je na tako negativnu ocenu.

D. Pregled celokupne analize sigurnosti domaćih veb sajtova

TABELA 1: PREGLED PRIMENE RAZLIČITIH TIPOVA ENKRIPCIJE I PROTOKOLA ANALIZOM DOMAĆIH VEB SAJTOVA BANAKA U SRBIJI

Naziv banke	Protokol					Algoritam								POODLE	FS	HSTS	OCENA
	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	DHE	ECDHE	RSA	AES	CBC	GCM	RC4	SHA				
Mobi banka						P				P							B
Raiff. banka						P				P							B
Halk banka						P				P							B
Credit Agricole						P					P						B
OTP banka						P				P							B
Kom. banka						P				P							B
SBER banka							P			P							A
Pošt. štedionica						P				P		P					F
Addiko banka						P					P						A^+
MTS banka						P					P	P					C
Unicredit						P				P							A^+
Banca Intesa						P				P							B
Erste banka						P				P							B
Procredit							P			P							A
AIK banka						P				P							B

U Tabeli 1 prikazan je pregled celokupne analize domaćih veb sajtova banaka. U okviru analize ispitano je koji se tačno protokoli koriste, algoritmi za enkripciju, takođe da li su sajtovi ranjivi na POODLE napade, da li je podržana FS – *Forward Secrecy* i u kojoj meri (da li sa svim pretraživačima ili samo nekim), kao i da li serveri podržavaju HSTS funkcionalnost. Takođe,

poslednja stavka u tabeli je konačna ocena na koju utiču svi prethodno navedeni faktori.

Tamno narandžastom bojom označeni su potpuno nesigurni elementi, svetlo naranžastom slabije sigurni, a zelenom bojom označeni su sigurni elementi. Slovo „P“ u tabeli označava da je neki algoritam podržan ali se retko koristi. Za svaki veb sajt banke označeni su **protokoli** koji se koriste (SSL 3.0 kao nesiguran protocol zbog ranjivosti na mnoge napade, u primeru analize predstavljen POODLE napad, TLS 1.0 i 1.1 kao slabo sigurni protokoli i TLS 1.2 i 1.3 kao jedni od najsigurnijih verzija protokola.), kao i **algoritmi** koji čine paket šifri za enkripciju (u tabeli su označeni kao skup algoritama za svaku banku u pogledu najčešće korišćenih prilikom simulacije rukovanja, npr. zeleno označena kombinacija algoritama predstavlja siguran paket šifri). Takođe, prikazano je koji veb sajtovi podržavaju RC4 protočnu šifru obzirom da postoji velika verovatnoća za zloupotrebu iste (napad na RC4 moguć je zbog statističkih propusta u nizu ključeva generisanih algoritmom koji otkriva delove šifrovanih poruka, pod uslovom da napadač može pribaviti dovoljno uzoraka za analizu). Prikazano je i na kojim serverima je implementirana HSTS funkcionalnost koja je od velikog značaja za zaštitu od napada „čovek-u-sredini“

Na isti način u Tabeli 2, prikazani su elementi analize sigurnosti domaćih veb sajtova onlajn prodavnica.

TABELA 2: PREGLED PRIMENE RAZLIČITIH TIPOVA ENKRIPCIJE I PROTOKOLA ANALIZOM DOMAĆIH VEB SAJTOVA ONLAJN PRODAVNICA U SRBIJI

Naziv prodavnice	Protokol					Algoritam								POODLE	FS	HSTS	OCENA
	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	DHE	ECDHE	RSA	AES	CBC	GCM	RC4	SHA				
KP						P				P							B
BUZZ						P				P							B
Kupindo						P				P							B
Tehnomanija						P				P							B
Forma Ideale						P				P							A

LITERATURA

[1] William Stallings, "*Osnove bezbednosti mreža*", CET, Beograd, 2014.
[2] Thyla van der Merwe, "*An Analysis of the Transport Layer Security Protocol*", University of London, 2018.
[3] Dr Stanislav Polić, "*Zaštita podataka u Internet okruženju*", Beograd, 2006.
[4] https://en.wikipedia.org/wiki/Transport_Layer_Security
[5] https://en.wikipedia.org/wiki/HTTPS

ABSTRACT

In addition to the significant contribution of modern technologies and the Internet in the banking sector, as well as in the sales sector, it is of great importance to determine their negative effects. Despite the constant struggle to keep security and privacy in the field of e-business as high as possible, the rise of cybercrime undermines trust and affects an increasing number of concerned users. Along with the adoption of new technologies, it is necessary to develop methods of protection against cybercrime in order for service users to be safe.

In this paper, we will present the negative effects of the application of modern technologies in electronic business, as well as how they can be overcome by using different types of encryption and protocols. We will also present a detailed overview of the security analysis of the websites of banking institutions in Serbia, as well as some well-known domestic online stores.

SECURITY ANALYSIS OF DOMESTIC WEBSITES

Ema Sinđelić