DOI: 10.19279/TVZ.PD.2017-5-1-11

KRIPTOGRAFSKI PROTOKOL

CRYPTOGRAPHY PROTOCOL

Ninoslav Ceglec[1], Dubravko Žigman[2]

[1]Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska, Student
[2]Tehničko veleučilište u Zagrebu, Zagreb, Hrvatska

Sažetak

Sadržaj ovoga članka detaljno objašnjava TLS protokol. Kroz članak je napravljena analiza izvedbe protokola i prikaz kako ga koristiti kako bi izvukli maksimum njegovih mogućnosti. Poseban naglasak ovoga članka stavljen je na slabosti protokola kako bi lakše shvatili prijetnje u njegovom svakodnevnom korištenju. Uz obradu slabosti protokola objašnjavamo i mogućnosti obrane i njihovog izbjegavanja kako bi izbjegli potencijalne prijetnje. Cilj članka je približiti tehnologiju koja se koristi u svakodnevnom životu iako u većini slučajeva je nismo niti svjesni. S obzirom da je osnovna svrha protokola razmjena osjetljivih podataka želimo približiti ispravno korištenje kako bi se smanjila mogućnost ugrožavanja osjetljivih podataka. Također, analizom njegovih slabosti željeli bismo osvijestiti mane protokola i na taj način pridonijeti sigurnosti korištenja. Kroz prikaz mogućnosti korištenja željeli smo prikazati scenarije korištenja kao i pozitivne i negativne strane ovisno o slučaju korištenja.

Ključne riječi: *TLS, kriptografski, protokol*

Abstract

The content of this article gives a detail article, a protocol performance analysis was performed as well as an overview of how to use it to maximize its capabilities. A special emphasis on this article was put on the weaknesses of the protocol to help you understand the threats in its everyday use. In addition to dealing with weaknesses in the protocol, we also explain the possibilities of defense and how to avoid potential threats.

The aim of the article is to bring close the technology that is used in everyday life, although in most cases we are not aware of it. Since the basic purpose of the protocol is exchange of sensitive data protocols, we wanted to bring closer the correct use in effort to reduce the risk of vulnerable data being compromised. Also, by analyzing its weaknesses, we want to raise awareness of protocol shortcomings and thus contribute to the security of use. Through the display of usage options, we would like to show usage scenarios as well as the positive and negative side depending on the case of use.

Keywords: *TLS, cryptography, protocol*

1. Uvod

1. *Intoroduction*

U vrijeme Web-a 2.0 koji je postao svakodnevica razmjena podataka putem računalnih mreža postala je svakodnevna radnja. Kupnja putem Interneta, internet bankarstvo, cloudi e-mail servisi samo su neki od primjera koji su postali naša svakodnevica. Pri korištenju navedenih usluga dolazi do dijeljenja osobnih informacija. Promatrajući nesigurno okruženje u kojem se nalaze računalne mreže, koje uključuje

vati da će podaci biti zlorabljeni na velik broj različitih načina. Jedan od mogućih oblika zaštite navedene vrste podataka je korištenje TLS (Transport Layer Security) protokola. TLS je kriptografski protokol koji omogućava razmjenu sigurnosno osjetljivih podataka na siguran način putem nezaštićenih računalnih mreža. Cilj TLS protokola je omogućiti sigurnu komunikaciju server/klijent aplikacija putem računalnih mreža na način da su iste zaštićene od prisluškivanja i promjene podataka.

Korištenjem TLS protokola rješavamo dvije izuzetno bitne stvari gledajući sigurnosni aspekt: sigurni smo da smo spojeni na server s kojim želimo razmjenjivati podatke te podaci koje razmjenjujemo ne mogu se pročitati i nisu promijenjeni putem. Navedeno se ostvaruje korištenjem asimetrične i simetrične kriptografije.

2. Način rada
2. *Work principles*

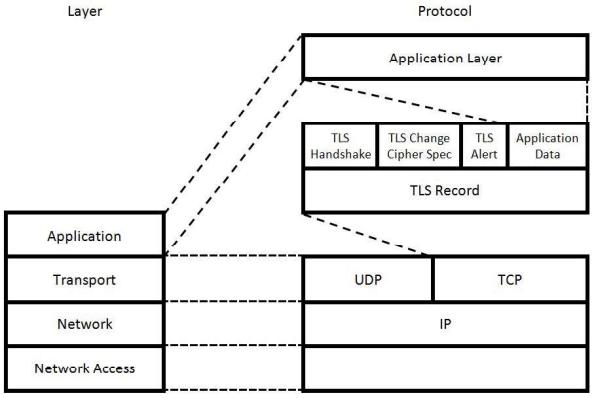
2.1. TLS protokol
2.1. *TLS cryptography protocol*

Za rad TLS protokola potrebno je u početku stvaranja veze odrediti tko je u vezi server, a tko klijent. Sigurnosnu komunikaciju uvijek pokreće klijent, dok server odgovara na zahtjev. TLS protokol, gledajući sa stajališta transportnog ili aplikativnog sloja, funkcionira kao jedna cjelina. Dubljim pogledom u protokol vidljivo je da se on sastoji od dvije vrste veza, dva pod sloja i pet pod protokola koji međusobno ovise i nadopunjuju se. Veze koje TLS protokol uspostavlja i koristi za sigurni protok podataka su TLS sesija i TLS konekcija.

TLS sesija koristi se za usklađivanje parametara potrebnih za uspostavljanje TLS konekcije. TLS sesija omogućava korištenje iste TLS sesija za više TLS konekcija. TLS konekcija koristi se za slanje podataka između dvije strane kriptološki zaštićenom vezom. Pod slojevi TLS protokola vežu se na protokole koji su neposredno iznad ili ispod njih. Niži od dva pod sloja veže se na neki protokol transportnog sloja poput TCP/IP (Transmission Control Protocol/Internet Protocol) Ovaj pod sloj brine se za enkripciju i prijenos podataka. Viši od dva pod sloja brine se za uspostavljanje sigurne konekcije između klijenta i servera.

Sastoji se od četiri pod protokola. TLS Handshake pod protokol koristi se kako bi se klijent i server međusobno autentificirali i usuglasili parametre potrebne za komunikaciju. TLS Change Cipher Spec pod protokol omogućava da klijent i server mijenjaju svoja read i write stanja čime započinje korištenje prethodno dogovorenih kriptografskih parametara.

TLS Alert pod protokol omogućava izmjenu standardiziranih upozoravajućih poruka. TLS Application Data pod protokol omogućava komunicirajućim stranama razmjenu podataka putem nekog protokola aplikativnog sloja TCP/IP referentnog modela. [1]



Slika 1 *Smještaj pod slojeva i pod protokola TLS protokola u TCP/IP referentnom modelu. [1]*

Figure 1 *Accommodation of sub-layers and sub-protocols from the TLS protocol in TCP / IP reference model. [1]*

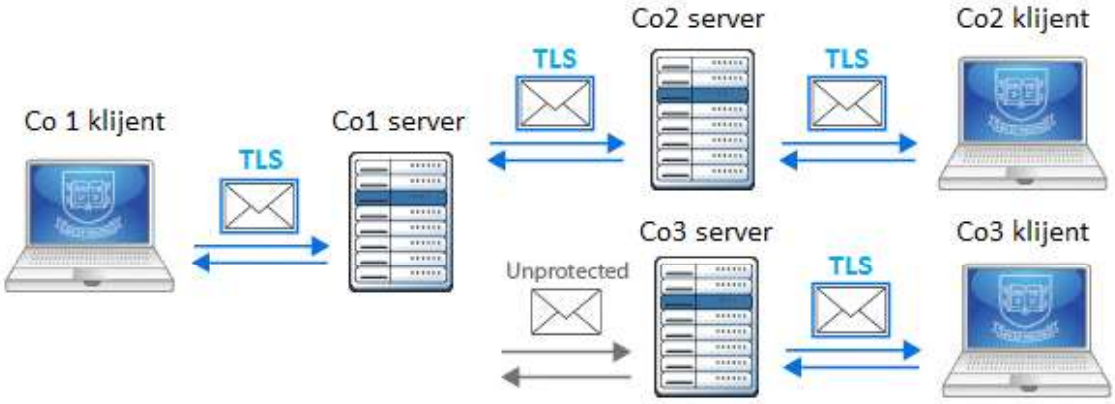
3. Korištenje, rasprostranjenost i implementacije TLS-a
3. *The use, distribution and implementation of the TLS*

3.1. Korištenje TLS-a
3.1. *The use of theTLS*

Neovisnost TLS-a o protokolu aplikacijskog sloja omogućuje njegovo korištenje s velikim brojem aplikacija. Generalno gledajući proces zaštite TLS-om svodi se na postavljanje sljedećih parametara: odluka o izboru strategije, aktiviranje upotrebe TLS-a na serveru, dodjela certifikata serveru te omogućavanje klijentu potvrdu certifikata servera.

3.1.1. E-mail zaštićen TLS-om
3.1.1. *E-mail protected by the TLS*

Kod zaštite e-mail poruka potrebno je naglasiti da TLS nije uvijek najbolje rješenje. Bez podešavanja svakog uređaja kroz koji poruka prolazi TLS ne pruža zaštitu e-mail-a od samog pošiljatelja do primatelja.



Slika 2 *E-mail s više primatelja*

Figure 2 *E-mail to multiple recipients*

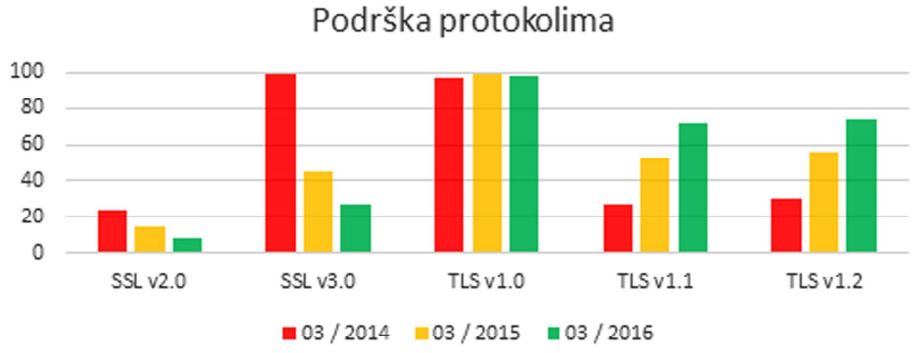
Slika 2 prikazuje slanje e-mail-a od strane Co1 klijenta koji šalje e-mail u dvije različite tvrtke. Jedna od tvrtki na svom serveru nema uspostavljenu TLS enkripciju prema vanjskom svijetu. Jasno je vidljivo da pri predaji poruke između servera Co1 i Co3 potencijalni napadač može bez većih problema doći do sadržaja e-mail poruke. Zaštita e-mail-a TLS-om ima i svojih dobrih strana. Gledajući iz perspektive krajnjeg korisnika, ne vidi se razlika između slanja zaštićenih ili nezaštićenih e-mail poruka. Nije potreban poseban e-mail klijent ili drugačije sučelje webmail-a da bi e-mail poruke bile zaštićene. TLS-om zaštićene e-mail poruke mogu se provjeravati na prisutnost virusa i spam-a te kontrolirati da li zadovoljavaju postavljenu sigurnosnu politiku subjekta. Na kraju do izražaja dolazi financijska strana u odnosu na druga rješenja koja nude slične usluge.

3.2. Rasprostranjenost i implementacije TLS protokola

3.2. *The distribution and implementation of the TLS*

Prednosti TLS protokola su njegova višestruka iskoristivost i mogućnost odabira između više implementacija. Objavljivanjem DTLS protokola mogućnosti korištenja dodatno su povećane. Loša strana velike rasprostranjenosti jest činjenica da otkrivanjem određene slabosti protokola dolazi do potencijalnog sigurnosnog utjecaja na gotovo svakog korisnika Interneta.

Slika 3 prikazuje rezultate istraživanja tvrtke SSL Labs vezane uz podršku TLS protokola na najpopularnijim zaštićenim web stranicama u razdoblju od 2 godine. Iz grafa je vidljivo da je najviše rasprostranjen protokol TLS verzije 1.0.



Slika 3 *Usporedba rasprostranjenosti verzija TLS protokola [4]*

Figure 3 *Comparison of distribution version of the TLS protocol [4]*

U ožujku 2016. godine oko 8% stranica još uvijek podržava SSL (Secure Socket Layer) v2.0, a 27% stranica SSL v3.0. Obje navedene verzije više se ne smatraju sigurnima te ih je potrebno izbjegavati. Prikazani pad podrške tim protokolima u razdoblju od 2 godine ukazuje na pozitivan trend odbacivanja nesigurnih verzija. Drugi pozitivan trend koji je moguće uočiti je značajno povećanje podrške za TLS verzije 1.1 i 1.2. Po prikazanim trendovima moguće je vidjeti pozitivnu stranu otkrivanja slabosti protokola, jer otkrivanjem slabosti podiže se svijest svih korisnika, što u konačnici pridonosi ubrzanju implementiranja novijih verzija protokola. [4]

4. Slabosti TLS-a
4. *TLS weaknesses*

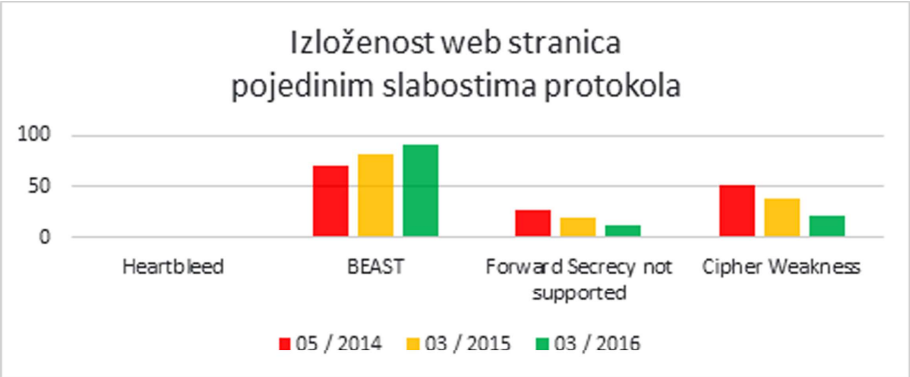
Ubrzo nakon pojavljivanja SSL-a 3.0 i uviđanja njegove vrijednosti u svijetu Interneta napravljena je detaljna sigurnosna analiza. Prvu neslužbenu sigurnosnu analizu proveli su David Wagner i Bruce Schneier koja je pokazala određene mane i teoretske mogućnosti napada, ali ukupna ocjena bila je pozitivna, s naglaskom da je SSL 3.0 važan doprinos praktičnoj zaštiti Internet komunikacije. [5]

Većina istraživanja slabosti TLS-a završava pronalaskom neke teorijske mogućnosti za razbijanje protokola ili nekog njegovog dijela. Svega nekoliko istraživanja dovelo je do praktičnih mogućnosti ugrožavanja sigurnosti TLS protokola. Važno je naglasiti da otkrivene slabosti protokola najčešće proizlaze iz nedovoljno dobre implementacije pravila postavljenih u standardu protokola.

Čitanjem dostupne literature dolazi se do zaključka kako unatoč otkrivenim slabostima generalni konsenzus pružatelja usluga je da postojeće stanje pruža zadovoljavajuću razinu sigurnosti te daje potencijalni rizik otkrivanja podataka prihvatljiv u odnosu na troškove koje donosi podizanje otpornosti na napade na najvišu moguću razinu.

Slika 4 prikazuje izloženost najpopularnijih web stranica prema najpoznatijim otkrivenim slabostima TLS protokola. Moguće je vidjeti da je Heartbleed u trenutku otkrivanja izazivao prijetnju prema samo 0,8% web stranica. Treba imati na umu kako je autor prilikom izrade testa bio ograničen kako ne bi došlo do otkrivanja osjetljivih podataka samim testom. Dodatni razlog ovakvih rezultata krije se u činjenici da je Heartbleed bio izuzetno dobro dokumentiran te je u iznimno kratkom roku većina izloženih servera „zakrpana“. [20]

Razlog početno visoke i povećavajuće izloženosti BEAST (Browser Exploit Against SSL/TLS) napadu nalazi se u analizi prikupljenih podataka. Sve stranice koje podržavaju algoritme s blokovskom enkripcijom (najpoznatiji primjer – AES (Advanced Encryption Standard)) smatraju se ranjivima, iako je praksa dokazala otklanjanje opasnosti ukoliko klijent koristi web pretraživač bilo koje verzije izdane nekoliko mjeseci nakon otkrivanja BEAST-a. Forward Secrecy not supported odnosi se na web stranice koje ne omogućuju Forward Secrecy, odnosno korištenje zasebnih ključeva za svaku konekciju između istog klijenta i servera.Cipher Weakness odnosi se na web stranice koje podržavaju nesigurne cipher suite-ove.



Slika 4 *Izloženost web stranica pojedinim slabostima protokola [4]*

Figure 4 *Exposure of websites to certain weaknesses of the protocol*

4.1. BEAST napad
4.1. *BEAST attack*

Istraživači Thai Duong i Julian Rizzo demonstrirali su u rujnu 2011. godine mogućnost probijanja SSL-a 3.0 i TLS-a 1.0 korištenjem BEAST napada koji su sami razvili. Slabost je povezana uz predvidljivo određivanje IV-a (Initialization Vector), a BEAST funkcionira kao napad odabranim otvorenim tekstom (chosen plaintext attack). [7, 8] Istraživanja su pokazala da je IV koji se koristi kod CBC (Cipher-Block Chaining) načina kriptiranja generiran po unaprijed poznatom i predvidljivom scenariju. Prilikom CBC kriptiranja koristi se IV kako bi se onemogućilo da dva ista bloka otvorenog teksta nakon kriptiranja i dalje budu ista. Pozitivna strana objavljivanja ovog napada je podizanje svijesti svih strana koje koriste Internet za razmjenu sigurnih podataka. Zahvaljujući BEAST-u jače je aktualizirano pitanje bržeg uvođenja novijih verzija TLS-a. BEAST napad funkcionira tako da napadač prvo mora podmetnuti BEAST aplikaciju u računalo klijenta kojeg želi napasti. Ona se sastoji od dva dijela: network sniffer-a i Javascript agenta koji ubacuje određeni otvoreni tekst u pakete.

Iako je pokazana praktična izvedivost napada potrebni su određeni uvjeti koje je u realnosti teško ispuniti poput:

- napadač mora klijentu podmetnuti BEAST aplikaciju
- napadač mora imati mogućnost nadzora prometa koji klijent radi
- aplikacija mora sadržavati Javascript kod koji omogućava generiranje i slanje poznatog teksta
- Javascript kod mora biti u mogućnost ubaciti poznati tekst na točno određeno mjestu u paketu
- klijent se mora tijekom trajanja napada prijaviti na određenu adresu
- napadač može dobiti kontrolu nad podacima klijenta pod uvjetom da klijent nije ugasio Internet pretraživač.

4.1.1. Zaštita od napada
4.1.1. *Protection from the attack*

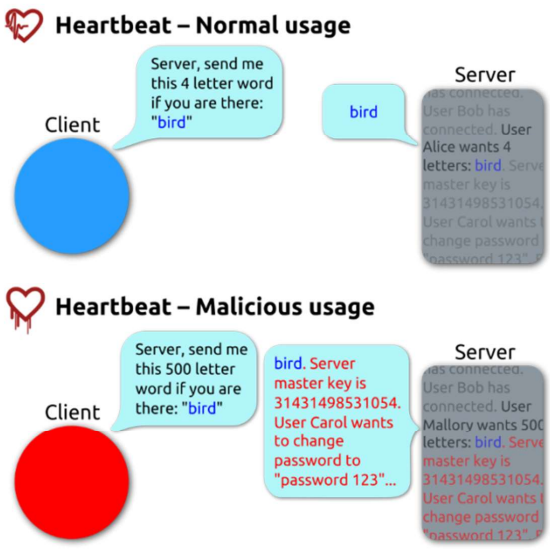
S administratorske strane jedina opcija svodi se na isključivo korištenje cipher suite-ova koji se baziraju na slijednoj enkripciji podržanoj od strane RC4 standarda. Pogledom na sliku 4 jasno je da se više od 90% administratora web stranica ipak odlučuje za blokovsku enkripciju zbog teorijske slabosti RC4 standarda. Krajnji korisnik ima na raspolaganju nekoliko mjera kojima se može zaštititi. Potrebno je naglasiti standardne savjete za izbjegavanje web sadržaja sumnjivog porijekla i nekorištenje nesigurnih LAN (Local Area Network) mreža prilikom rada s osjetljivim podacima poput Internet bankarstva i provjeravanja e-mail-a. Prilikom pristupa stranicama s povjerljivim sadržajem, preporuča se ponovo pokretanje internet pretraživača ukoliko je prije pretraživan Internet. Po završetku rada na spomenutima stranicama, potrebno je izvršiti odjavu s istih i ugasiti Internet pretraživač prije nastavka pretraživanja Interneta.

Jedna od mjera je i gašenje izvođenja Java koda u Internet pretraživaču ali problem je što određene stranice poput Gmail-a zahtijevaju izvođenje Java koda. [9]

4.2. Heartbleed
4.2. *Heartbleed*

U travnju 2014. godine odjeknula je dosad najpoznatija slabost TLS protokola popularno nazvana Heartbleed.Ona se odnosi na OpenSSL implementaciju TLS protokola, u konkretnom slučaju OpenSSL v1.0.1 do uključujući v1.0.1f. Izuzetan odjek Heartbleed-a prouzrokovan je iz dva glavna razloga. Prvi je činjenica o velikoj rasprostranjenosti OpenSSL implementacije, dok je drugi mogućnost napadača da dođe do kriptografskih ključeva koji mu omogućavaju dekripciju svih poruka razmijenjenih između dvije povezane strane. Uspoređujući sliku 5s drugim istraživanjem koje prikazuje da je 17% ispitanih servera (oko 500 000 servera) koji podržavaju TLS protokol u trenutku ispitivanja bilo podložno Heartbleed-u dobivamo dvosmislenu sliku opasnosti koju ova slabost predstavlja.

Razlika između prikazanih rezultata proizlazi u načinu ispitivanja; drugo istraživanje je usredotočeno na podržavanje heartbeat ekstenzije, glavnog uzročnika Heartbleed-a. [10]Za razliku od prethodno predstavljenih slabosti i napada u slučaju Heartbleed-a ugrožene su obje komunicirajuće strane, server i klijent. Heartbleed iskorištava heartbeat ekstenziju, uvedenu s OpenSSL-om v1.0.1. Heartbeat ekstenzija služi za održavanje TLS konekcija. Njezina primjena je zamišljena poglavito za DTLS protokol kako bi omogućila ispitivanja je li druga komunicirajuća strana prisutna i održavanje TLS konekcije u slučaju prekida prijenosa paketa s jedne strane. Heartbeat ekstenzija radi na način da jedna strana šalje heartbeat poruku koja se sastoji od određenog payload-a i dužine payload-a, dok je druga strana obvezna poslati isti payload natrag.



Slika 5 *Princip rada Heartbleed-a [11]*

Figure 5 *Work principles of the Heartbleed [11]*

Slika 5 prikazuje logičku pogrešku u kodu spomenutih verzija OpenSSL-a koja omogućuje Heartbleed slabost. Ona se odnosi na izostanak provjere veličine payload-a koji prozvana strana vraća prozivatelju. U konkretnom primjeru napadač šalje određenu poruku veličine 4 bita i kao veličinu paketa navede 500 bita. U tom slučaju prozvana strana odgovara porukom koja će se sastojati od 4 bita prvotne poruke i 496 bita koja proizlaze iz radne memorije prozvane strane. Najveći problem je što se svi osjetljivi podaci nalaze upravo u radnoj memoriji prozvane strane. Iako je veličina otkrivajućegpayload-a ograničena na 64 kB, nije ograničen broj upita odnosno paketa što osigurava uspjeh napada. [11] Heartbleed je prikazao paradoks koji donosi ažurno održavanje korištenih implementacija i korištenje zadnjih verzija TLS protokola. OpenSSL v1.0.1 donio je podršku za TLS verzije 1.1 i 1.2. i sustavi koji su ga brzo uveli postali su ranjivi zbog pogreške u implementaciji protokola.

4.2.1. Zaštita od Heartbleed-a

4.2.1. *Protection from the Heartbleed*

Prvo rješenje je korištenje OpenSSL implementacije v1.0.1g ili više. U spomenutim verzijama ispravljen je izvorni kod dodavanjem provjere veličine poslanog payload-a s upisanom veličinom istoga. Postoji i mogućnost ukidanja potpore za heartbeat ekstenziju dodavanjem OPENSSL_NO_HEARTBEATS zastavice u izvorni kod. Ukoliko se koristi neko sistemsko rješenje koje koristi sporne verzije OpenSSL-a potrebno je napraviti nadogradnju ponuđeno od strane proizvođača. Nakon toga potrebno je napraviti izmjenu svih podataka koji su potencijalno izloženi napadu poput privatnih i javnih ključeva i sve vezane certifikate, te poništiti postojeće certifikate. Nakon navedenih koraka, ukoliko se radi o serveru potrebno je promijeniti pristupne lozinke. Ukoliko korisnik smatra da se stranica kojoj pristupa putem TLS protokola nalazi na ugroženom serveru, potrebno je promijeniti pristupnu lozinku.[11]

5. Zaključak

5. *Conclusion*

Izbor TLS-a prisiljava prihvaćanje određenih kompromisa koje donose njegove dobre i loše strane. Potrebno je naglasiti da za veliku većinu usluga kojima je TLS namijenjen isti predstavlja najbolje rješenje zahvaljujući prevladavajućem popisu pozitivnih stvari. Iako teorija preporuča korištenje najnovijih verzija određenog protokola, praksa pokazuje da je ponekad potrebno koristiti zastarjele verzije koje imaju odličnu podršku.

Otkrivanjem određenih slabosti brzo se pojavljuje odgovarajuća zakrpa pa je potrebno pratiti događanja vezana uz verziju i implementaciju koja se koristi kako bi se na vrijeme reagiralo. Prikazana istraživanja ukazuju na sporo uvođenje novih verzija protokola koje bi ispravnim implementiranjem podigle razinu sigurnosti. Razlog se krije u financijama koje bi iziskivale uvođenje novosti u postojeći sustav i rasprostranjenost starijih verzija protokola te vezana inertnost Internet zajednice. Dokaz kvalitete TLS-a je razvoj DTLS-a kojima se povećavaju mogućnosti korištenja. Na kraju je potrebno naglasiti da TLS protokol sam po sebi ne pruža potpunu sigurnost. Kako bi TLS dao svoj maksimum u zaštiti osjetljivih podataka i njihovih korisnika, potrebno je unaprijed odrediti ciljeve koje želimo zadovoljiti te na temelju istih pravilno odabrati verzije TLS-a i pripadajuće implementacije. Nakon navedenog koraka potrebna je pažljiva konfiguracija i održavanje, čime se dobiva odlično rješenje za siguran prijenos sigurnosno osjetljivih podataka putem nesigurnih računalnih mreža.

5. Reference

5. *References*

[1] Oppliger,R.: „SSL and TLS; TheoryandPractice“, Artech House, Boston, 2009. godine.

[2] Modadugu, N.;Rescorla, E.:„The Design and Implementation of Datagram TLS“, SAD, 2006. godina.

[3] Risitić, I.: „Bulletproof SSL and TLS“, Feisty Duck Limited, Ujedinjeno Kraljevstvo, 2014. godina.

[4] URL: https://www.trustworthyinternet.org/ssl-pulse/(14.03.2016.)

[5] URL: http://www.schneier.com/paper-ssl-revised.pdf(14.03.2016.)

[6] URL: http://www.cs.berkeley.edu/~daw/my-posts/netscape-cracked-0(16.03.2016.)

[7] URL: http://eprint.iacr.org/2004/111(16.03.2016.)

[8] URL: http://www.openssl.org/~bodo/tls-cbc.txt(16.03.2016.)

[9] URL: http://en.wikipedia.org/wiki/Transport_Layer_Security(16.03.2016.)

[10] URL: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (17.03.2016.)

[11] URL: https://en.wikipedia.org/wiki/Heartbleed (17.03.2016.)

AUTORI · *AUTHORS*

Dubravko Žigman - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 1, No. 1, 2013.

Korespodencija

dzigman@tvz.hr

Ninoslav Ceglec - Student Tehničkog veleučilišta u Zagrebu.

Korespodencija

nino.ceglec@gmail.com