SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1759

Analiza protokola za upravljanje sigurnosnim certifikatima

Dominik Petrović

Zagreb, travanj 2018.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu `\izvornik`.

hvala?

SADRŽAJ

1. Uvod

Uvod rada. Nakon uvoda dolaze poglavlja u kojima se obrađuje tema.

2. Teorijska pozadina

U prvom poglavlju ovog rada opisuju se SSL (eng. *Secure Sockets Layer*) i TSL (eng. *Transport Layer Security*) tehnologije korištene u sigurnosti pri prijenosu osjetljivih podataka u komunikaciji između sustava. Ostatak poglavlja pruža uvod u kriptografiju.

2.1. SSL, TLS i Kriptografija

Svakim danom svijet postaje sve više povezan. Tijekom zadnjeg stoljeća popularnost Interneta eksponencijalno je narasla i time promijenila naše živote. Već sada je broj pametnih mobitela veći od broja ljudi. Također, sve više se umrežuju čitavi informatički sustavi, industrijska postrojenja i mnoge druge tehnologije. Navedene primjene i uređaji koji ih koriste imaju zajedničku poveznicu - oslanjaju se na protokolima zvanima SSL i TLS, kako bi zaštitili informacije u prijenosu.

2.1.1. Transport Layer Security

U fazama razvoja Interneta i procesa umrežavanja, fokus nije bio usmjeren na sigurnost. Rezultat toga je da su temeljni komunikacijski protokoli inheretno nesigurni i temelje se na međusobnom povjerenju svih uključenih stranki. Takav pristup je bio moguć u ranim fazama umrežavanja, ali danas je neostvariv i predstavlja problem.

TSL i njegov prethondik SSL su kriptografski protokoli razvijeni u svrhu stvaranja sigurnosne komunikacije u nesigurnom okruženju (infrastrukturi). Pravilnom implementacijom SSL I TSL protokola moguće je stvoriti sigurni komunikacijski kanal s proizvoljnim servisima na Internetu ili nekoj drugoj mreži, biti siguran da je ostvarena komunikacija s odgovarajućim serverom i da će izmjena informacija biti ostvarena na siguran način. Ovi protokoli štite *transportni sloj*, odakle TLS i dobiva ime.

Sigurnost nije jedini cilj TLS protokola. Naime, ima četiri glavna cilja, poredana u listu po prioritetima:

- **Kriptografska sigurnost** - glavni problem je omogućiti sigurnu komunikacija između bilo kojih stranki koje žele ostvariti izmjenu informacija.
- **Interoperabilnost** (međusobno funkcioniranje) - nezavisni programeri trebaju moći razviti programe i biblioteke koje mogu međusobno komunicirati koristeće uobičajene kriptografske postupke.
- **Protežnost** - TLS efektivno predstavlja okvir za razvoj i implementaciju kriptografskih protokola. Važno je da su međusobno nezavisni o korištenim kriptografskim primitivima, pritom dozvoljavajući migraciju jednog primitiva drugom bez potrebe za stvaranjem novih protokola.
- **Efikasnost** - zadnji cilj predstavlja ostvarivanje svih gore navedenih ciljeva u prihvatljivom okvirima performansa, minimizirajući izdatke performansa kriptografskih operacija i pružajući plan predmemoriranja (cacheing) trenutne sesije.

2.1.2. Mrežni sloj

Internet je u svojoj osnovi temeljen na IP i TCP protokolima, koji se koriste za pakiranje podataka u pakete za transport. Paketi prolaze kroz mnoge mreže i informatičke sustave (nazvane *hops*) i budući da osnovni protokoli ne pružaju nikakvu sigurnost sami po sebi, svatko s pristupom komunikacijskom sloju može dobiti puni pristup informacijama i podacima u tranzitu, a tako i promijeniti čitavi promet bez ikakvog otkrivanja.

IP i TCP nisu jedini ranjivi protokoli. Postoji čitavi opseg protokola korištenih za **routing** - omogućavanje računalima da pronađu tražene servise na mreži. Servisi kao DNS su jedni od njih, a veza namjenjena jednom računalu može biti odgovorena neočekivane stranke.

Kako bi se podaci i informacije osigurale, koriste se enkripcijski postupci. Napadač može pogledati enkriptirane podatke, ali ne može ih dekriptirati i modificirati po želji. U spriječavanju takvih napada, SSL i TSL se oslanjaju na PKI-u (eng, *Public-key Infrastructure*), koji osigurava da se mrežni promet šalje odgovarajućem primatelju.

U svrhu razumijevanja kako se SSL i TSL uklapaju, potrebno je razmotriti OSI (eng. *Open Systems Interconnection*)model. OSI oredstavlja konceptualni model korišten u opisivanju mrežne komnukacije. Ukratko, sva funkcionalnost je mapirana u sedam slojeva:

Tablica 2.1: Slojevi OSI modela

	OSI sloj	Opis	Protokol primjer
7	Applkacijski	Aplikacijski podaci	HTTP, SMTP, IMAP
6	Prezentacijski	Prikaz podataka, konverzija, ekripcija	SSL/TLS
5	Sesija	Upravljanje višestrukim konekcijama	-
4	Transportni	Pouzdano dostavljanje paketa	TCP, UDP
3	Mrežni	Usmjeravanje i dostavljanje datagrama između mrežnih node-ova	IP, IPSec
2	Podatkovni	Pouzdana lokalna podatkovna konekcija (LAN)	Ethernet
1	Fizički	Izravna fizička konekcija	CAT5

Najniži sloj je najbliži fizičkoj komunikacijskoj vezi; naredni slojevi su grade nad prethodnim slojevima i pružaju višu razinu apstrakcije. Na samome vrhu se nalazi aplikacijski sloj, koji nosi aplikacijske podatke. Strukturiranje komunikacije na ovaj način pruža uredno razdvajanje implementacije; protokoli se ne moraju birnuti o funkcionalnosti implementiranoj u nižim slojevima. Nadalje, protokoli u različitim slojevima mogu biti dodani i maknuti; protokoli u nižim slojevima mogu biti korišteni za mnoge protokole u višim slojevima.

SSL i TSL su odličan primjer kako taj princip funkcionira u stvarnosti. Nalaze se iznad TCP-a, ali ispod protokola više razine kao HTTP. Kada enkripcija podataka nije potrebna, TSL se može ukloniti iz modela, bez utjecaja na

2.1.3. Kriptografija

Kriptografija ima mnogo definicija, ali u ovom radu kriptografiju opisuje znanost i umjetnost sigurne komunikacije. Kada se kriptografija pravilno primjeni, adresira tri temeljna zahtjeva sigurnosti:

- Čuvanje tajni (*confidentiality*)
- Verificiranje identiteta (*authenticity*)
- Osiguravanje sigurnog prijenosa podataka (*integrity*)

Kriptografija je veoma raznoliko područje i ima snažne temelje u matematici, ali u svrhu ovog rada, pregled kriptografije će se držati na visokoj razini s ciljem ostvarivanja osnovnih razumijevanja za daljnje shvaćanje rada.

2.1.4. Građenje blokova

Kritpografija na svojoj najnižoj razini se zasniva na korištenju raznih kriptografskih primitiva. Kriptografski primitivi su dobro uhodani low-level kriptografski algoritmi korišteni za građenje kriptografskih protokola gdje je svaki primitiv posebno dizajniran s određenom korisnom funkcionalnošću. Primjerice, možemo koristiti primitive za enkripciju i drugi primitiv za provjeru cjelovitosti. Primitivi posebno nisu veoma korisni, ali njihove kombinacije u sheme i protokole pružaju otporni sigurnosne sustave.

Tko su Alice i Bob?

Alice i *Bob* su imena najčešće korištena u raspravama vezanim za kriptografiju. Koriste se kako bi inače suhoparnu temu učinili zanimljivijom. Zasluge za prvo korištenje tih imena pripadaju Ronu Rivestu, koji je u svom radu 1977 koristio ta imena za predstavljanje RSA kriptosistema. U ovome radu su predstavljeni i korišteni Finn, kao uljez s mogućnošću prisluškivanja komunikacije i Jake, kao uljez s mogućnošću posredovanja mrežnog prometa.

2.1.5. Simetrična enkripcija

Simetrična enkripcija (eng. *Symmetric encryption* ili *Private-key cryptography*) je metoda enkripcije koja omogućuje sigurni prijenos upreko nesigurnog komunikacijskog kanala. Kako bi mogli sigurno komunicirati, Alice i Bob se prvo trebaju složiti oko enkripcijskog algoritma i *tajnog ključa*. Kada Alice odluči poslati željene podatke Bobu, koristi tajni ključ kako bi enkriptirao podatke. Bob koristi isti ključ kako bi ih dekriptirao. Jake, uljez s pristupom komunikacijskom kanalu, može vidjeti podatke, ali ne može ih dekriptirati i vidjeti originalne podatke. Alice i bob mogu proizvoljno dugo nastaviti sigurnu komunikaciju, ako drže tajni ključ sigurnim.

Enkripcija podataka se provodi dugi niz godina, primjerice *zamjenskim šifriranjem* (eng. *substitution cipher*). Prije pojašnjenja što je zamjensko šifriranje, potrebno je objasniti što je *šifrirani tekst* (eng. *ciphertext*) i *dekripcija*(eng. *decryption*). U kriptografiji, šifrirani tekst je rezultat enkripcije provedeno nad običnim textom, koristeći algoritam, često zvan šifra(eng. *cipher*). Šifrirani tekst je također poznat kao enkriptirana infomracija iz razloga što sadrži oblik originalnog texta, koji je nečitljiv drugima bez odgovarajuće šifre. Dekripcija, inverzan postupak enkripcije, je proces prevođenja

šifriranog teksta u čitljivi originalni tekst postupkom iverzne šifre.
Zamjensko šifriranje je metoda enkripcije u kojoj se *jedinice* (eng. *units*) čitljivog texta zamjenjuju nekom drugom jedinicom (primjerice slovo abecede drugim slovom abecede) i pritom čine šifrirani tekst. Primatelj šifriranog teksta dekriptira primljeni tekst inverznom ekripcijom.

Put a pikčr koji sam napraviš

U iznad opisanoj metodi ne koristi se sigurnosni ključ, što predstavlja raniji pristup ekripciji. Danas je usvoj drugačiji pristup temeljen na opažanju kriptografa 19. stoljeća, *Augustea Kerckhoffsa*:

"A cryptosystem should be secure even if the attacker knows everything about the system, except the secret key".

Kerckhoffovo načelo je usvojeno iz nekoliko razloga:

- Da bi enkripcisjki algoritam bio koristan, mora biti dijeljiv s drugima. Kako raste broj osoba s pristupom algoritmu, vjerojatnost da će agoritam postati nesiguran također raste.
- Pojedinačni algoritam bez sigurnosnog ključa je nepraktičan za korištenje u velikim grupama; svatko može dekriptirati tuđu komunikaciju.
- Veoma je mučan proces dizajnirati dobar enkripcijski algoritam. Sigurnost algoritma raste s njegovim ispitivanjem i izlaganjem različitim scenarijima. Preporuča se konzervativan pristup prilikom usvajanja novog algoritma. Obično se godinama pokušava razbiti algoritam kako bi se utvrdila sigurnost šifre.

Dobar enkripcijski algoritam je onaj koji izdaje naizgled nasumičan šifrirani tekst, pritom ne otkrivajući nikakve informacije originalnog teksta, što onemogućuje napadaču analizu.

2.2. PKI

3. Protokoli

4. Programska izvedba

5. Simulacija i analiza eksperimentalnih rezultata

6. Zaključak

Zaključak.

LITERATURA

Analiza protokola za upravljanje sigurnosnim certifikatima

Sažetak

Sažetak na hrvatskom jeziku. alala

Ključne riječi: Ključne riječi, odvojene zarezima.

Title

Abstract

Abstract.

Keywords: Keywords.