



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
-STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Goran Anđelković
SSL, bezbednosni propusti i zaštita
- Master rad -

Mentor:
Prof. dr Mladen Veinović

Student:
Goran Anđelković
Br. indeksa: 410039/2010

Sažetak

U cilju postizanja najvišeg nivoa zaštite komunikacija, profesionalni sistemi moraju razviti sopstvene sisteme zaštite, otporne na sve poznate tipove napada. Međutim profesionalni sistemi prinuđeni su i na balans između funkcionalnosti i zaštite korisnika. Svoje usluge postavljaju na poznatu infrastrukturu i u najvećem broju slučajeva štite SSL protokolom uz korišćenje podataka koji su korisniku poznati (korisničko ime i lozinka). Na ovaj način postignut je balans između funkcionalnosti i zaštite, zanemarujući pravila bezbednosti i autentifikacije za nečim što korisnik ima i nečim što korisnik jeste.

U ovom radu su objašnjeni, u cilju realizacije jake autentifikacije u informacionim sistemima sa zatvorenom grupom korisnika, zaštite na transportnom nivou u cilju sprečavanja eksternih napada na informacione sisteme.

U savremenim računarskim mrežama, kao mehanizam zaštite na transportnom nivou, najčešće se primenjuje standardni SSL (Secure Sockets Layer) protokol (novija verzija je TLS (Transport Layer Security) protokol) između korisnika i web servera (ili web servisa).

Ključne reči – bezbednost računarskih mreža, zaštita transportnog sloja mreža, HTTPS, SSL protokol, TLS protokol

Abstract

In order to achieve the highest level of security, professional communication systems have developed their own systems of protection, resistant to all known types of attacks. However, professional systems and are forced to balance between functionality and user protection. The services are placed at known infrastructure in most cases protected by SSL protocol to use data that has been known to user (username and password). In this way, there has been a balance between functionality and security, ignoring the rules of security and authentication for something that user has and something the user is.

This paper explains, in order to implement strong authentication in information systems with a closed group of users, the transport layer in order to prevent external attacks on information systems.

In modern computer networks, as a mechanism for the transport level, the most commonly applied standard SSL (Secure Sockets Layer) protocol (newer version of the TLS (Transport Layer Security) protocol) between the user and the web server (or web service).

Keywords - computer network security, network transport layer security, HTTPS, SSL protocol, TLS protocol

Sadržaj

1. Uvod	4
2. Prethodna istraživanja	5
3. Metodologija istraživačkog projekta	7
3.1. Predmet istraživanja	7
3.2. Ciljevi i zadaci istraživanja	7
3.3. Istraživačke hipoteze	8
3.4. Metode i tok istraživačkog procesa	9
3.5. Struktura rada	9
4. Bezbednost informacija.....	11
5. Istorijat	12
6. Osnovni principi bezbednosti informacija	13
6.1. Poverljivost.....	13
6.2. Integritet	14
6.3. Dostupnost.....	14
6.4. Autentičnost.....	14
6.5. Neporicanje.....	15
7. Računarske mreže	16
7.1. Vrste računarskih mreža	16
7.1.1. LAN	16
7.1.2. WAN.....	16
7.2. OSI model.....	16
8. Osnove bezbednosti u računarskim mrežama	22
8.1. Bezbednost i zaštita servisa računarskih mreža.....	23
8.2. Pristupi bezbednosti mrežnog saobraćaja.....	23
8.3. Zaštita na transportnom nivou	25
9. SSL protokol	28
9.1. Arhitektura SSL-a.....	29
9.1.1. SSL protokol evidencije	31
9.1.2. Specijalni protokol za promenu šifrata.....	34
9.1.3. Protokol upozorenja.....	34
9.1.4. Protokol sinhronizacije	35

10. HTTPS	37
10.1. Iniciranje veze	37
10.2. Zatvaranje veze.....	38
11. Slabosti SSL protokola.....	39
11.1. Korisnička ubeđenja i pretpostavke.....	39
11.2. Lista organizacija za izdavanje potvrda	40
11.3. Napad prisluškivanjem saobraćaja	40
11.4. Napad zaobilaženjem sigurne veze	41
11.5. Napad ubacivanjem potvrda	42
11.6. Cipher suite - povratni napad	42
11.7. Problem male dužine ključeva.....	43
11.8. Nedostatak HTTPS uspostave veze.....	43
11.9. Uspostavljanje SSL veze	44
12. SSL aplikacije	46
12.1. SSL bazirane virtuelne privatne mreže (VPM)	46
12.2. On-line plaćanje kreditnim karticama	47
12.3. S-HTTP i SSL.....	49
13. Predložena rešenja za SSL protokol.....	50
14. Zaključak.....	51
Literatura	52

1. Uvod

Nagli razvoj tehnologije računarskih sistema i mreža, doveo je do masovne razmene informacija i podataka. U toj razmeni pojavila se potreba za zaštitom poverljivih podataka od raznih krađa i zloupotreba, što je uslovalo pojavu novog pravca u oblasti bezbednosti podataka. Dalji razvoj tehnologije doprineo je poboljšanju karakteristika metoda koje doprinose bezbednosti podataka. Međutim, isti taj napredak doveo je do bržeg otkrivanja nedostataka i dodatno omogućio eventualne zloupotrebe. Tako su, tokom vremena, metode za zaštitu podataka postajale sve složenije i naprednije.

Popularnost Interneta, i njegovih korisnika je u rastu svaki dan, i broj korisnika koji koriste elektronske transakcije raste isto tako. Takođe, popularnost SSL aplikacija upućuje na opasnost od otkrivanja i iskorišćavanja sigurnosnih "rupa" u protokolu, koji bi mogli ugroziti sigurnost podataka koji se štite. SSL je vrlo jeftin za implementaciju, i razvijen je kao brza solucija za potrebe sigurnosti u web aplikacijama, koje rade sa poverljivim podacima. To objašnjava više implementacija ovog protokola na Internetu.

U radu je predstavljen i analiziran SSL protokol, i njegova primena u savremenim računarskim mrežama. Analizirane su savremene metode zaštite i ukazano je na njihove nedostatke. Kriptografski protokoli čine osnovicu svih protokola za zaštitu podataka koji se implementiraju na višim nivoima.

Cilj ovog rada je da ukaže na nužnost zaštite podataka i prikaže osnovne mehanizme za njihovu zaštitu, koji se prenose putem računarske mreže. Zbog fizičkih i funkcionalnih karakteristika računarskih mreža, veoma često se javlja opasnost od ugrožavanja podataka prilikom prenosa. Predmet istraživanja rada je upoznavanje sa metodama koje se danas koriste da onemoguće zloupotrebu podataka. Pregledom najčešće korišćenih algoritama za kriptovanje, tehnika za autentifikaciju, problema prilikom upravljanja sa ključevima i sigurnosnim servisima u TCP/IP modelu, saznaju se osnove o zaštiti podataka. Uporednom analizom karakteristika određenih metoda za zaštitu ukazuje se na prednosti i/ili nedostatke. U cilju što efikasnijeg prikaza složenih procedura upotrebljen je veliki broj praktičnih primera i ilustracija.

2. Prethodna istraživanja

Sa brzim razvojem mrežnih aplikacija, problem bezbednog prenosa postaje veoma važan. Zbog toga je SSL protokol sve više u širokoj upotrebi u različitim mrežnim servisima. Ovaj protokol sam po sebi nije savršen i u praksi sa njim često postoje problemi. Ovaj deo rada ukazuje na problem koji postoji u procesu SSL uspostavljanja veze. Prva mana kod uspostavljanja veze je što se u početnoj fazi koristi otvorena komunikacija pa postoji mogućnost neovlašćenog praćenja sadržaja. Druga mana je implementacija SSLa u aplikaciju. Zbog razmatranja faktora o radu mrežne veze, obično se koristi prekidač veze zasnovan na HTTP protokolu koji prebacuje saobraćaj na HTTPS.

Na primenu SSL-a značajno utiču i razvoj e-trgovine i rad u „oblaku“. Njegovom primenom garantuje se bezbednost komunikacionog procesa, a koriste se mehanizmi autentifikacije od kraja do kraja, šifrovanje poruka, provera integriteta poruke i drugi mehanizmi zaštite. Najveći svetski proizvođači koriste SSL kako bi štitili svoje klijente. Primera radi, Google štiti sigurnost razmene mailova kao i prijave svojih korisnika preko SSL protokola. Poslednjih par godina značajan rast beleži i korišćenje sistema rada u „oblaku“. Razmena podataka se u najvećem broju slučajeva obavlja putem SSL protokola. VeriSign, kao najveće autorizaciono telo za izdavanje SSL sertifikata, čak garantuje sigurnu uslugu svim korisnicima nove Microsoft Windows Azure platforme u „oblaku“ [2]. Kada se radi u „oblaku“ svi podaci korisnika i sva obrada podataka obavlja se na udaljenoj lokaciji pa je samim tim neophodno da veza funkcioniše savršeno, ali i da ostane bezbedna kako ne bi došlo do kompromitovanja podataka. Bankarski sektor je napadačima najzanimljiviji ali i sektor na koji su korisnici usluga najosetljiviji i gde očekuju najveću bezbednost. Savremeno elektronsko bankarstvo se uglavnom oslanja na SSL protokol kao odgovarajući model zaštite.

Ipak pokazalo se da SSL nije savršen za svaki tip primene. Još 2003. realizovani su napadi na SSL protokol i dokazane su greške u uspostavljanju veze koje su omogućavale napad preuzimanja sesije. U 2009. godini Michael Howard je uspešno realizovao napad korišćenjem alata Webmitm [1] – alat za Linux okruženje koji uspešno dešifruje podatke iz SSL protokola. Iste 2009. godine na internacionalnoj bezbednosnoj konferenciji predstavljeno je rešenje koje prosleđuje saobraćaj sa HTTPS na HTTP saobraćaj koji se dalje mnogo lakše obrađuje i prisluškuje. Kod ovih napada klijenti ne primećuju razliku u uslugama i servisima koje koriste.

Proizvođači Internet pretraživača unapređivali su zaštitu svojih klijenata koja se zasniva na upozorenjima na nevalidne sajtove kao i na lažne sertifikate. Kompanije za antivirusna rešenja razvile su rešenja za zaštitu od ARP prevara, koja se najčešće koriste pri napadima. Međutim, pored svih zaštita i inicijativa proizvođača programa često su nastajali bezbednosni propusti koji se i danas koriste.

Ovaj rad bazira se na analizi bezbednosnih propusta koji se javljaju pri SSL uspostavljanju veze. Analiza je rađena primenom dva metoda. Prvi metod zasniva se na karakteristikama otvorenog teksta u fazi uspostavljanja veze kao nedostatku klijent sertifikacione autentifikacije, preuzimanju sesije preko ARP obmane i DNS poplave u okviru mrežnog segmenta. Napadač podmeće falsifikat serverskog sertifikata i predstavlja se kao proksi ili gateway nakon čega dolazi u mogućnost za napad. Posledica je da napadač može da dešifruje sve podatke prenete putem https-a. Drugi metod zasniva se na korišćenju

defekta SSL-a i zaobilaženja istog u praktičnoj primeni. Na početku se ARP prevarom napadač predstavlja kao lažni proksi ili gateway. Napadač uspostavlja HTTPS vezu sa pravim serverom i ta komunikacija se dalje obavlja sa pravim sertifikatom, dok se veza za obmanutim klijentom obavlja preko HTTP saobraćaja čiji je saobraćaj lako pratiti i obrađivati. Napadač direktno šalje otvoren tekst klijentu sa HTTP strane dešifrovanjem šifrovanih podataka, tako da on može da pristupi svim komunikacijama podataka.

U eksperimentalnoj analizi obrađeno je u odnosu na specifičnosti nekoliko napada po prethodno opisanim scenarijima. Analizirani su verovatnoća uspeha napada i mogućnost klijenta da primeti da je do napada uopšte i došlo. Nakon eksperimenata obavljene su i dva kursa obuke, nakon kojih su rađene analize obučanih klijenata za detekciju napada i predstavljeni su rezultati grupe pre i nakon obuke.

3. Metodologija istraživačkog projekta

Projektni zadatak ima za cilj da analizira, prikaže i definiše pojmove i procese u protokolima zaštite računarskih mreža, i da nam ukaže na nedostatke. U radu se posebno ističe značaj modeliranja ovih procesa prema odgovarajućim standardima i specifikacijama.

Oslonac u izradi teksta ovog rada čine teoretska znanja iz oblasti informaciono-komunikacionih tehnologija, ali i praktična znanja i istraživanja na polju kriptografije i zaštite računarskih mreža.

U ovom poglavlju biće reči kako o predmetu istraživanja, tako i o ciljevima i zadacima istraživanja, gde se na osnovu postavljenih ciljeva koriste određene metode. Ovo istraživanje je podržano saznanjima iz međunarodne naučne i stručne literature.

3.1. Predmet istraživanja

Predmet istraživanja ovog rada su osnovni principi zaštite savremenih računarskih mreža, kao i osnovni protokoli koji se pri tome koriste.

Predmet istraživanja rada je upoznavanje sa metodama koje se danas koriste da onemoguće zloupotrebu podataka. Pregledom najčešće korišćenih algoritama za kriptovanje, tehnika za autentifikaciju, problema prilikom upravljanja sa ključevima i sigurnosnim servisima u TCP/IP modelu, saznavaju se osnove o zaštiti podataka.

U radu se razmatra više međusobno povezanih problema:

1. Analiza aktuelnih napada na elektronsku i ličnu svojinu
2. Istraživanje zaštite koju nudi SSL
3. Nedostaci HTTPS uspostavljanja veze
4. Napadi na HTTPS saobraćaj
5. Predlog rešenja za odbranu od napada

3.2. Ciljevi i zadaci istraživanja

Cilj ovog rada je da ukaže na nužnost zaštite podataka i prikaže osnovne mehanizme za njihovu zaštitu, koji se prenose putem računarske mreže. Zbog fizičkih i funkcionalnih karakteristika računarskih mreža, veoma često se javlja opasnost od ugrožavanja podataka prilikom prenosa. Uporednom analizom karakteristika određenih metoda za zaštitu ukazuje se na prednosti i nedostatke. U cilju što efikasnijeg prikaza složenih procedura upotrebljen je veliki broj praktičnih primera i ilustracija.

3.3. Istraživačke hipoteze

Hipoteze koje čine osnovu ovog rada su:

1. U uslovima globalizacije poslovanja, jake konkurentnosti i promenljivosti okruženja, elektronsko poslovanje sve više dobija na važnosti i neophodnosti. Obezbeđivanje sigurne komunikacije nameće se kao imperativ uspešnog obavljanja elektronskih transakcija.
2. Primena i usvajanje elektronskog poslovanja u Republici Srbiji, direktno će zavisiti od stepena poverenja klijenata u sigurnost i bezbednost obavljenih transakcija.
3. Uspešnost primene elektronskog poslovanja i elektronskih transakcija u direktnoj je korelaciji sa kvalitetom procesa njegovog projektovanja, sprovođenja i bezbednosti.

Posebne hipoteze:

1. Bankarsko tržište kao najreprezentativniji korisnik elektronskih transakcija predstavlja jak kontrolni mehanizam zaštite sigurne komunikacije, intenzivno promoviše upotrebu elektronskih transakcija radi ostvarenja boljih poslovnih i finansijskih performansi.
2. Uspešnost obezbeđivanja sigurnog elektronskog poslovanja je u direktnoj korelaciji sa redovnom kontrolom i revizijom informacionih sistema i sistema zaštite komunikacije.
3. Od ekonomske snage privrednih subjekata direktno zavisi uvođenje i pravilna primena novih tehnologija.

3.4. Metode i tok istraživačkog procesa

Metodološki pristup istraživanja koji će se primenjivati u izradi ovog istraživanja postavljen je veoma kompleksno i zahteva primenu:

- od analitičkih osnovnih metoda: metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- od sintetičkih osnovnih metoda: sintezu, konkretizaciju, generalizaciju i indukciju;
- od opšte naučnih metoda: hipotetičko - deduktivnu, analitičko - deduktivnu, komparativnu, statističku i metodu modelovanja.

Adekvatna primena ovog pristupa omogućiće da se steknu pouzdana saznanja o predmetu istraživanja, o činjenicama, pojavama, procesima i odnosima na kojima počiva i odvija se transformacija internet bankarstva, ali i o pojmovima, stavovima, sudovima i zaključcima koji su relevantni za ispunjavanje svrhe ovog rada.

3.5. Struktura rada

Rad se sastoji od 14 poglavlja, podeljenih prema materiji koja se u njima obrađuje.

U prvom poglavlju dat je uopšteniji i kraći opis celokupnog rada. Određene su izvesne podele prema kojima je ovaj rad i usmeren.

U drugom poglavlju je izložena problematika prethodnih radova, svrha i značaj istraživanja, kao i definicije najvažnijih termina i objašnjenje korišćenih metoda.

U trećem poglavlju je data metodologija naučnog istraživanja, koja podrazumeva, predmet, ciljeve i zadatke naučnog istraživanja, kao i metode i tok istraživačkog procesa.

U četvrtom poglavlju je predstavljena bezbednost informacija kao zaštita informacija i informacionih sistema od neautorizovanog pristupa, korišćenja, razotkrivanja, remećenja, izmene ili uništenja.

Peto poglavlje prikazuje kako se je kroz istoriju razvijala potreba za pronalaženjem nekih od mehanizama za zaštitu poverljivosti pisanih dokumenata i sposobnost otkrivanja sertifikata.

U šestom poglavlju dati su osnovni principi bezbednost informacija, koje održava poverljivost, integritet i dostupnost, kao svoje osnovne principe.

U sedmom poglavlju su opisane vrste računarskih mreža, kao i OSI referentni model.

U osmom poglavlju opisani su načini zaštita servisa računarskih mreža, kao i pristupi bezbednosti mrežnog saobraćaja.

Deveto poglavlje, opisuje Secure Sockets Layer (SSL), 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 aplikacijski sloj.

U desetom poglavlju se ukazuje na značaj HTTPS-a (HTTP preko SSL), koji se odnosi na kombinaciju HTTP i SSL protokola kako bi se implementirala sigurna komunikacija između veb pretraživača i mrežnog servera.

Jedanaesto poglavlje predstavlja okosnicu rada, i ukazuje nam na slabosti SSL protokola. SSL je vrlo jeftin za implementaciju, i razvijen je kao brza solucija za potrebe sigurnosti u web aplikacijama, koje rade sa poverljivim podacima. To objašnjava više implementacija ovog protokola na Internetu. Međutim, kao i svaki drugi sistem, SSL nije u potpunosti siguran.

U dvanaestom poglavlju su prikazane neke od SSL aplikacija koje koriste banke ili pojedine kompanije, a koje pružaju razne usluge svojim klijentima.

Trinaesto poglavlje prikazuje kako su se uz SSL razvijala su se neka rešenja koja ostvaruju zaštićeni prenos podataka kroz mrežu. Uspešnost SSL-a dodatno je naglašena nedostatkom drugih dovoljno dobrih rešenja koji bi ga zamenili. U ovom poglavlju su dati kraći pregledi nekih od rešenja.

U četrnaestom poglavlju, tj. zaključku, dat je kraći opis celokupnog rada.

4. Bezbednost informacija

Bezbednost informacija predstavlja zaštitu informacija i informacionih sistema od neautorizovanog pristupa, korišćenja, razotkrivanja, remećenja, izmene ili uništenja.

Bezbednost informacija, računarska bezbednost i osiguranje informacija često se mešaju iako se u suštini radi o različitim stvarima. Ove oblasti su međusobno povezane i imaju sličnu namenu da zaštite poverljivost, integritet i dostupnost informacija međutim među njima postoje i ozbiljne razlike.

Ove razlike leže pre svega u pristupu subjektu, metodologiji korišćenja i temama koje pokrivaju. Bezbednost informacija je povezana sa pojmovima kao što su poverljivost integritet i dostupnost podataka bez obzira na formu u kojoj se ti podaci nalaze: elektronska, štampana ili neka druga forma dok je računarska bezbednost fokusirana na osiguravanje dostupnosti i ispravno funkcionisanje računarskog sistema bez osvrta na informacije koje se skladište ili obrađuju na računaru.

Vlade, vojska, korporacije, finansijske institucije, bolnice i privatni biznis poseduju veliku količinu poverljivih informacija o svojim zaposlenima, kupcima, proizvodima, istraživanjima i finansijskoj situaciji. Veliki broj ovih informacija se sada uz pomoć računara prikupljaju, obrađuju i skladište a zatim se tako pripremljeni šalju preko mreže prema drugim računarima.

Treba li da poverljive informacije o kupcima, finansijama ili liniji novih proizvoda padnu u ruke konkurenciji što bi uz probijanje bezbednosnih mera moglo da dovede do propasti posla, sudskog postupka ili čak i stečaja kompanije. Zaštita poverljivih informacija je na prvom mestu poslovna ali takođe i etička kao i pravna stvar.

Za pojedinca, bezbednost informacija može da ima bitne posledice na privatnost na koju se veoma različito gleda u različitim kulturama.

Oblast bezbednosti informacija značajno je rasla i razvijala se u novije vreme. Ova oblast takođe pruža niz mogućnosti za razvoj uspešne karijere, jer zahteva razne vrste specijalizacija. Specijalnosti kao što su obezbeđivanje mreže odnosno mreža i sličnih infrastruktura, obezbeđivanje aplikacija i baza podataka, testiranje bezbednosti, revizija informacionih sistema, digitalna forenzika samo su neka od zanimanja koja se mogu sresti u ovoj oblasti.

5. Istorijat

Još od najranijih dana korišćenja pisma državne vođe i vojni komandanti razumeli su neophodnost pronalaženja nekih od mehanizama za zaštitu poverljivosti pisanih dokumenata i sposobnost otkrivanja sertifikata. Osobe koje su želele bezbednu komunikaciju koristili su pečat od voska i druge načine pečačenja da potvrde autentičnost dokumenta, spreče falsifikovanje i obezbede poverljivost korespondencije.

Julije Cezar je stekao ugled sa izumom “Cezarove šifre” 50-te godine p.n.e. koja je stvorena sa ciljem da predupredi da njegove tajne poruke budu pročitane ukoliko dospeju u pogrešne ruke.

Drugi svetski rat je doneo mnoge novine u oblasti bezbednosti informacija i označio je početak profesionalnog bavljenja ovom oblašću. Uočene su prednosti fizičke zaštite informacija sa barikadama i naoružanim stražama koje kontrolišu pristup u informatičke centre. Takođe je uvedena klasifikacija podataka bazirana na njihovoj osetljivosti kao i identifikacija osoba koje mogu da pristupe informaciji. Tokom Drugog svetskog rata takođe se sprovodila provera porekla pre dobijanja prava na klasifikovanje informacija.

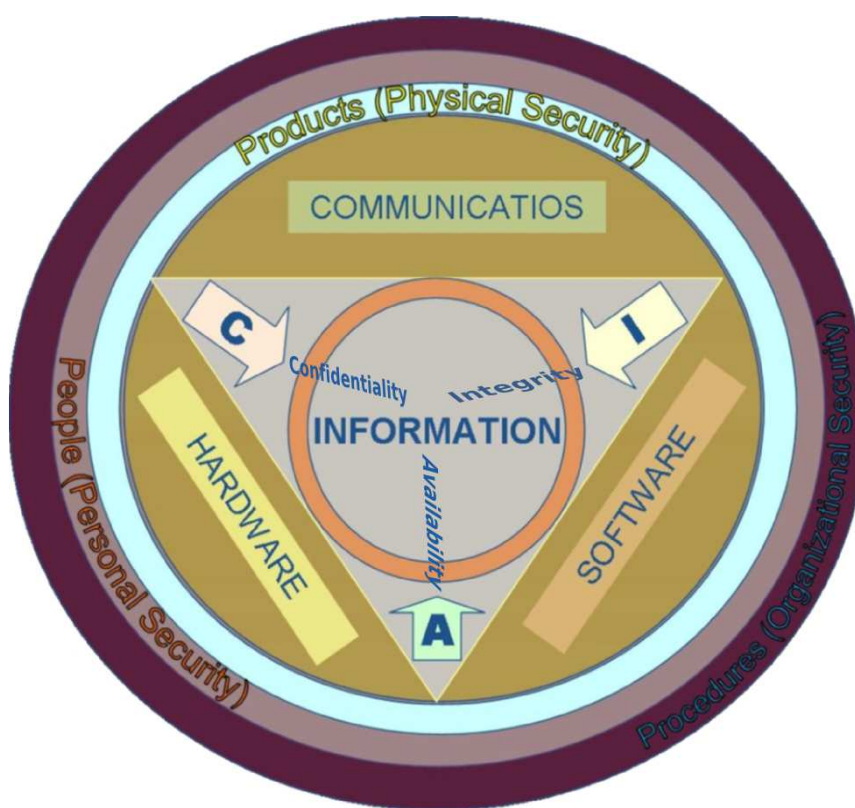
Kraj 20-og i početak 21-og veka povezan je sa brzim razvojem telekomunikacija, računarskog hardvera i softvera i šifrovanje podataka. Manje, snažnije i dostupnije računarske komponente učinile su elektronsku obradu podataka bližom malim i srednjim preduzećima kao i kućnim korisnicima. Ubrzo su ovi računari postali povezani unutar mreže koja se naziva Internet ili World Wide Web.

Brz porast i široka upotreba elektronske obrade podataka i elektronskog poslovanja koje se sprovodi preko Interneta, među sve brojnijim pojavama međunarodnog terorizma, zahteva bolje metode zaštite računara i informacija koje su na njima uskladištene, obrađene i prosleđene. Akademske discipline računarske bezbednosti, bezbednosti informacija i informatička sigurnost izdvajaju se među brojnim profesionalnim organizacijama koje dele isti cilj obezbeđivanja sigurnosti i pouzdanosti informacionih sistema.

6. Osnovni principi bezbednosti informacija

Bezbednost informacija održava poverljivost, integritet i dostupnost poznatiju kao CIA trojstvo (confidentiality, integrity and availability), kao svoje osnovne principe. Informacione sisteme možemo da raščlanimo na tri osnovna dela hardver, softver i komunikacije sa ciljem da identifikujemo i primenimo industrijske standarde za bezbednost informacija kao mehanizme za zaštitu i prevenciju u tri sloja i to: fizički sloj, personalni sloj i organizacioni sloj.

Ukratko, procedure i politike su implementirane da objasne zaposlenima (administratorima, korisnicima i operaterima) kako da koriste proizvode da bi obezbedili sigurnost informacija unutar organizacije.



Slika 1. Komponente koje obezbeđuju bezbednosti informacija

6.1. Poverljivost

Poverljivost podrazumeva sprečavanje razotkrivanja informacija neautorizovanom pojedincu ili sistemima. Na primer transakcije kreditnim karticama preko Interneta zahtevaju da kupac svoj broj kreditne kartice treba da prezentuje trgovcu, nakon čega trgovac prenosi broj kreditne kartice banci koja će da izvrši autorizaciju. Poverljivost se štiti šifrovanjem broja kreditne kartice tokom prenosa, ograničavanjem broja mesta gde može da se pojavi (baze podataka log fajlovi, backup, štampani izveštaji i slično), kao i ograničavanjem

pristupa mestima gde se skladište. Ako neko ko nije autorizovan dobije broj kreditne kartice, na bilo koji način, dolazi do narušavanja poverljivosti.

Narušavanje poverljivosti se može realizovati na više načina. Dopustivši neke pogled preko ramena na monitor vašeg računara dok su na njemu prikazane osetljive informacije predstavlja narušavanje poverljivosti. Krađe ili prodaja laptopa koji sadrži poverljive podatke o zaposlenima iz kompanije može rezultirati narušavanjem poverljivosti. Izdavanje poverljivih informacija putem telefona je takođe narušavanje poverljivosti ukoliko poziv dolazi od osobe koja nije autorizovana da primi te informacije. Poverljivost je neophodna za očuvanje privatnosti osoba čiji se lični podaci čuvaju na sistemu.

6.2. Integritet

U okviru bezbednosti informacija, integritet podrazumeva da se podaci ne mogu menjati bez procesa autorizacije, što ne treba mešati sa referencijalnim integritetom kod baza podataka. Integritet je narušen kada zaposleni nenamerno ili zlonamerno izbriše važne podatke, kada virus inficira računar, kada je zaposleni u mogućnosti da menja sopstvenu zaradu u bazi podataka platnih spiskova, kada neautorizovani korisnik uništi Web sajt, kada neko može da odbaci veliki broj glasova prilikom online glasanja i tako dalje.

Postoji mnogo načina u kojima je integritet ugrožen bez zle namere. Najjednostavniji primer je kada korisnik prilikom unosa podataka nepravilno unese nečiju adresu. Nešto kompleksniji je slučaj kada automatizovani proces nije pravilno napisan i testiran, pa proces ažuriranja baze podataka može da izmeni podatke na neodgovarajući način ugrožavajući time integritet podataka. Profesionalci koji se bave ovom oblašću pokušavaju da pronađu načine za implementaciju kontrole koje će preduprediti ugrožavanje integriteta.

6.3. Dostupnost

U svakom informacionom sistemu informacija mora da bude dostupna kada se za njom ukaže potreba. To zapravo znači da računarski sistemi skladište i obrađuju podatke, bezbednosni sistemi ih štite, a funkcionalni komunikacioni kanali omogućavaju pristup. Visoko dostupni sistemi imaju za cilj da budu dostupni sve vreme sprečavajući prekid usluge koju računar pruža čak i u slučaju gubitka napajanja, kvara na hardveru ili nadogradnje sistema. Osiguranje dostupnosti takođe uključuje sprečavanje denial-of-service napada.

Godine 2002., Donn Parker predlaže alternativni model za klasično CIA trojstvo koji je nazvao “Šest atomskih elemenata informacija”. Ovi elementi su poverljivost, posedovanje, integritet, autentičnost, dostupnost i upotrebljivost. Vrednost Parkerove heksade je predmet rasprave među profesionalcima koji se bave bezbednošću sistema.

6.4. Autentičnost

U računarstvu, e-poslovanju i bezbednosti informacija neophodno je da se obezbedi da podaci, transakcije, komunikacije ili dokumenti (elektronski ili materijalni) ostanu

izvorni. Za autentičnost je takođe važna validacija koja omogućava da obe uključene strane treba da dokažu da su ono što tvrde da jesu.

6.5. Neporicanje

U pravnim naukama, neporicanje povlači nečiju nameru da izvrši svoju obavezu prema ugovoru. To takođe implicira da jedna strana u transakciji ne može da porekne prijem transakcije niti druga strana može da porekne slanje transakcije.

Elektronska trgovina koristi tehnologiju digitalnog potpisa i šifrovanje kojima postiže autentičnost i neporicanje.

Upravljanje bezbednošću podrazumeva sledeće aktivnosti:

- Procesi
- Politike , standardi, procedure, uputstva
- Upravljanje rizicima
- Kontrole
- Tehnologija
- Dokumentacija IT sistema
- IT kultura
- Edukacija

7. Računarske mreže

7.1. Vrste računarskih mreža

7.1.1. LAN

Lokalna računarska mreža ili LAN (engl. Local Area Network - LAN) je skup računara koji su povezani u jednu računarsku mrežu, na relativno malom prostoru, kao što su kancelarija, više kancelarija ili zgrada.

Ova mreža može da broji dva i više računara koji su povezani na određen način. Neki periferni uređaji kao što su štampači, modemi i sl., takođe se ubrajaju u ovu mrežu. Glavna karakteristika lokalnih mreža, po čemu se one razlikuju od mreža na velikim područjima (WAN) jeste mnogo veća brzina prenosa podataka (reda 10 do 1000 MB/sec) i nepostojanje potrebe za zakupljenim telekomunikacionim vodovima.

Najčešći metod povezivanja računara u lokalnoj mreži jeste kablovima (Ethernet) ili bežična mreža. Lokalna mreža može, najčešće preko nekog rutera, biti povezana sa drugim mrežama u veću WAN mrežu ili direktno preko provajdera na Internet.

7.1.2. WAN

Regionalna računarska mreža ili akronim WAN od (engl. Wide Area Network) (Računarska mreža širokog područja u slobodnom prevodu) je računarska mreža koja pokriva šire područje - grada, regiona ili države. Ponekad se izraz WAN koristi za mrežu koje koristi rutere i javne komunikacione veze.

Regionalna mreža se koristi za povezivanje različitih lokalnih računarskih mreža tako da omogućuje komunikaciju između korisnika i računara u različitim mrežama. WAN se gradi za potrebe jedne ili više kompanija ili pojedinca ili za potrebe internet provajdera koji je koriste kako bi omogućili pristup internetu lokalnim mrežama i pojedinim računarima. Može biti izgrađen pomoću iznajmljenih mreža koji preko rutera povezuju više lokalnih mreža ili lokalnoj mreži omogućavaju vezu za Internet. Kako su iznajmljene linije prilično skupe za WAN se često koristi neki od sistema komutiranja paketa. Mrežni protokoli, kao što su TCP/IP omogućavaju transport i adresne funkcije.

7.2. OSI model

Krajem 70-tih godina, međunarodna organizacija za standardizaciju (Internacional Organization for Standardization, ISO), je kreirala referentni model, Open System Interconnection (OSI) da bi računari različitih proizvođača mogli da komuniciraju. OSI model je bio namenjen da pomogne proizvođačima u kreiranju kompatibilnih mrežnih uređaja i softvera u formi protokola. Opisuje kako jedna aplikacija na jednom računaru, kroz mrežni medijum, saopštava podatke i mrežne informacije aplikaciji na drugom računaru. Referentni model predstavlja sve procese potrebne za uspešnu komunikaciju i deli sve procese u logičke grupe – slojeve. Ovako dizajniran model se naziva slojevita arhitektura.

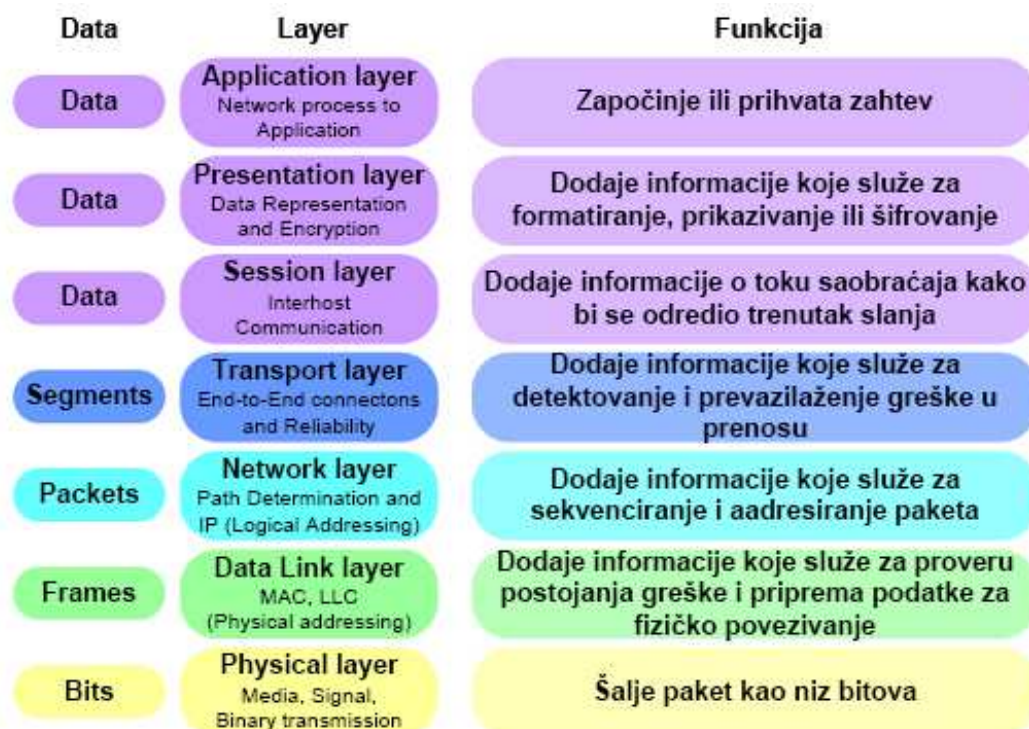
OSI model je hijerarhijski model i treba da omogući mrežama različitih proizvođača da rade zajedno.

Prednosti korišćenja OSI slojevitog modela su:

- Deli komunikacione procese u mreži na manje i jednostavne komponente
- Omogućava višeproizvođački razvoj kroz standardizaciju mrežnih komponenti
- Omogućava različitim vrstama mrežnog hardvera i softvera da rade zajedno
- Sprečava da izmene na jednom sloju utiču na druge slojeve, tako da se ne ometa razvoj

OSI model se sastoji od 7 odvojenih, ali međusobno povezanih slojeva kroz koje moraju da prođu podaci na svom putu od izvišta preko mreže do odredišta. Čine ga sledeći slojevi:

7. sloj – sloj aplikacije (application layer)
6. sloj – sloj prezentacije (presentation layer)
5. sloj – sloj sesije (session layer)
4. sloj – sloj transporta (transport layer)
3. sloj – sloj mreže (network layer)
2. sloj – sloj veze (data link layer)
1. sloj – fizički sloj (physical layer)



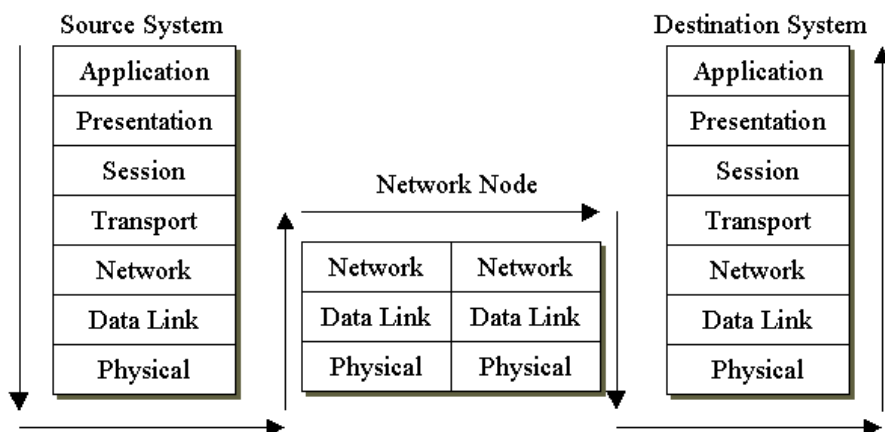
Slika 2. OSI referentni model

OSI model ima 7 slojeva zbog toga što su se njegovi tvorci povelili u to vreme, daleko najvećim proizvođačem računara, firmom IBM, koja je za svoje mreže koristila sedmoslojni protokol SNA (System Network Architecture). U OSI modelu osnovna su 3 koncepta: koncept usluge, interfejsa i koncept protokola.

Unutar jednog računara svaki sloj zahteva usluge od sloja ispod sebe. Procesi (entiteti) koji se nalaze u istom sloju, ali na različitim računarima nazivaju se entiteski parovi ili ravnopravni entiteti. Entiteski parovi prividno direktno komuniciraju – svaki sloj u izvorišnoj stanici prividno komunicira sa odgovarajućim slojem u odredišnoj stanici. Komunikacija između entiteskih parova obavlja se pomoću jednog ili više protokola datog sloja. Protokol je skup pravila koji upravlja načinom na koji 2 entiteta razmenjuju podatke.

Virtuelna komunikacija između odgovarajućih slojeva u izvoričnom i u odredišnom računarima obavlja se pomoću njima odgovarajuće protokolske jedinice podataka (PDU – Protocol Data Unit). U stvarnosti podaci se ne prenose direktno iz sloja N jednog računara u sloj N drugog već svaki sloj šalje podatke i upravljačke informacije u sloj neposredno ispod sebe sve dok se ne dostigne najniži sloj. Ispod fizičkog sloja je medijum kroz koji se odvija stvarna komunikacija. Na prijemu, pristigli podaci ulaze u fizički sloj i sukcesivno prolaze kroz slojeve dok se ne stignu u sloj aplikacije.

Jedinica podataka sloja transporta naziva se SEGMENT, sloja mreže PAKET, sloja veze RAM ili OKVIR, a jedinica fizičkog sloja je BIT.



Slika 3. Prikaz prolaska podataka kroz OSI model

Sloj aplikacije

Sloj aplikacije omogućava korisniku (čoveku ili programu) da pristupi mreži. Zato ovaj sloj sadrži niz protokola koji su potrebni za pružanje podrške raznovrsnim uslugama: elektronska pošta, pristup fajlovima, www, diskusione grupe, pričaonica... Sloj aplikacije se ponaša kao kao interfejs između stvarnog aplikacionog programa, koji nije deo slojevite strukture, i sledećeg sloja ispod, pružajući načine da aplikacija pošalje informacije naniže kroz stek protokola. Npr IE se ne nalazi unutar sloja aplikacije, već komunicira sa protokolima sloja aplikacije.

Važno je da se razume da u OSI modelu aplikacija ima različito značenje od onog značenja koje ima u standardnoj računarskoj terminologiji. U OSI modelu sloj aplikacije obezbeđuje servise koje koristi korisnička aplikacija. Kada se na korisničkom računaru

pokrene neka aplikacija kao što je na primer Web pretraživač ona se ne nalazi u sloju aplikacije već samo koristi servise koje joj isporučuje protokol koji radi u sloju aplikacije i koji se zove the Hypertext Transfer Protocol (HTTP). Razlika između Web pretraživača i HTTP protokola je mala, ali je ipak bitna.

Sloj prezentacije

Ovaj sloj se bavi sintaksom i semantikom informacija koje razmenjuju dva sistema. Ovaj sloj je odgovoran za:

- Prevođenje
- Šifrovanje
- Kompresiju
- Jedini menja podatke
- Prevodi podatke
- Šifrue podatke

Pre prenosa, informacija se mora pretvoriti u nizove bitova. Različiti računari koriste različite sisteme kodovanja za predstavljanje alfanumeričkih podataka (ASCII, UNICODE), celih brojeva (komplement jedinice, komplement dvojke). Da bi se omogućila komunikacija između procesa koji za predstavljanje informacija koriste različite kodove, neophodno je obaviti prevođenje kodnog sistema koji se koristi u izvoru u kodni sistem koji se koristi u odredištu. To se postiže na sledeći način:

- U sloju prezentacije predajnika, informacija se iz formata koji se koristi unutar predajnika konvertuje u neki opšti format
- U sloju prezentacije prijemnika obavlja se inverzna operacija: opšti format se prevodi u format koji se koristi u tom prijemniku

Kada se zahteva tajnost podataka, mora se obaviti šifrovanje podataka (data encryption). Šifrovanje se obavlja u predajniku tako što konvertuje originalnu poruku u drugačiji oblik i tek onda šalje na mrežu. Cilj kompresije je da smanji broj bitova koji se prenose, a da se sačuva prenešena informacija.

Sloj sesije

Termin sesija (session) označava period komuniciranja tj vođenja dijaloga između procesa (programa). Sloj sesije ima zadatak da uspostavi, održava i sinhronizuje komunikaciju između 2 sistema. Ima dva osnovna zadatka:

- Upravljanje dijalogom
- Sinhronizacija

Sloj sesije koordinira komunikacijom između 2 sistema i služi da organizuje njihovu komunikaciju tako što nudi tri različita režima: SIMPLEKS, POLUDUPLEKS, PUNI DUPLEKS. Ako se saobraćaj u sistemu odvija u jednom smeru, sloj sesije vodi računa o tome ko emituje u određenom trenutku.

Drugi zadatak sloja sesije je da u poruku unese sinhronizacione tačke. To su kontrolne tačke koje se unose na određenom rastojanju. Ako dođe do prekida prenosa, prenos se nastavlja od poslednje sinhronizacione tačke.

Sloj transporta

Sloj transporta je odgovoran za isporuku cele poruke s kraja na kraj veze tj od izvorišta do odredišta. Osnovni zadatak sloja transporta je da:

- Prihvata podatke iz sloja sesije
- Podeli ih, ako treba na manje jedinice
- Propusti ih u sloj mreže
- Osigura da svi delovi poruke stignu na drugi kraj

U sloju transporta se obavlja sledeće:

- SAP adresovanje – adresovanje tačaka pristupa uslugama ili adresovanje portova; dok sloj mreže dovodi svaki paket u odredišni računar, sloj transporta dovodi celu poruku u odredišni računar
- Rastavljanje (segmentacija) i ponovno sastavljanje: poruka se deli na segmente koji se mogu preneti i svakom segmentu se dodeljuje redni broj kako bi sloj transporta u odredištu moga da prispele pakete identifikuje i složi po ispravnom rasporedu, zamenjujući pakete koji su se tokom prenosa zagubili njihovim ponovo poslatim kopijama
- Upravljanje konekcijom: sloj transporta može da bude konekciono orijentisan (connection-oriented) ili beskonexioni (connectionless)
- Upravljanje protokom
- Kontrola grešaka

Sloj mreže

Sloj mreže nadzire isporuku paketa, a sloj transporta nadzire isporuku cele poruke. Sloj mreže je neophodan ako su dve stanice koje se nalaze u različitim mrežama koje su povezane uređajima koji se nazivaju ruteri. On je odgovoran za:

- Logičko adresiranje: fizičko adresiranje (koje se obavlja u sloju veze) dovoljno je kada se računari nalaze u istoj mreži, u protivnom sloj mreže unosi u zaglavlje paketa logičke adrese izvorišta i odredišta
- Određivanje putanje odnosno rutiranje
- Kontrola zagušenja

Sloj veze

Ovaj sloj je zadužen za:

- Formiranje ramova: na otpremi dodaje paketu pristiglom iz sloja mreže zaglavlje i rep
- Fizičko adresovanje: u zaglavlje rama unosi fizičku adresu predajnika i fizičku adresu prijemnika
- Upravljanje protokom: ako je brzina kojom predajnik prihvata podatke manja od brzine kojom predajnik šalje podatke, sloj veze aktivira mehanizam za upravljanje protokom kako bi se sprečilo da brzi predajnik zaguši spori prijemnik
- Kontrolu grešaka: pomoću informacija u repu rama, omogućava otkrivanje grešaka
- Upravljanje pristupa medijumu

Fizički sloj

U fizičkom sloju se ram podataka koji stiže iz sloja veze konvertuje u nestruktuiran niz bitova. Zbog toga se fizički sloj bavi mehaničkim i električnim specifikacijama interfejsa i medijuma za prenos i definiše postupke i funkcije koje fizički uređaji i interfejsi moraju da obavljaju tokom prenosa. Zadaci fizičkog sloja su:

- Mehanička pitanja vezana za pristup medijumu
- Električna pitanja vezana za pristup medijumu
- Proceduralna pitanja vezana za pristup medijumu

Fizički sloj je zadužen za:

- Definisanje karakteristika interfejsa između uređaja (računara) i medijuma za prenos
- Definisanje vrste medijuma za prenos
- Predstavljanje bitova pomoću električnih ili optičkih signala
- Određivanje trajanja bita tj brzina emitovanja
- Vremensku sinhronizaciju tj sinhronizaciju predajnika i prijemnika na nivou bita
- Definisanje smeru prenosa (simpleks, poludupleks, dupleks)
- Način umrežavanja računara: da li se radi o topologiji u obliku magistrale, zvezde, prstena ili svako sa svakim.

8. Osnove bezbednosti u računarskim mrežama

U ranim fazama razvoja tehnologija na kojima se baziraju računarske mreže fokus je bio postavljen na omogućavanje što veće brzine prenosa podataka sa što manjom verovatnoćom greške. Mala baza korisnika, sastavljena uglavnom od tehnički obrazovanih korisnika, i retke praktične primene omogućile su brz razvoj tehnologija i dovele računarske mreže do potencijala kojim prete da u potpunosti zamene ostale popularne sisteme komunikacije kao što su telefonija i televizija. Međutim, rastom popularnosti računarske mreže su izašle iz čisto tehničko-tehnološkog domena i sve više na njihov razvoj i primenu imaju ekonomski i socijalni faktori.

Internet, kao najveću računarsku mrežu danas, koriste milioni korisnika putem velikog broja dostupnih servisa. Putem ove mreže se prenose lični podaci korisnika, obavljaju poverljive poslovne video-konferencije i razgovori, obavljaju finansijske transakcije, prenose poverljive vojne i državne informacije, obavljaju udaljeni hirurški zahvati i još mnogo toga. Stoga, na primeru Interneta možemo zaključiti da se putem računarskih mreža sve više prenose vrednosti realnog sveta, često daleko veće nego što je to slučaj kod telefonije i televizije. Međutim, svaka vrednost sa sobom nosi najčešće srazmeran rizik koga je, kako u realnom tako i u virtuelnom svetu računarskih mreža, cilj eliminisati ili u što većoj meri umanjiti. Postizanje ovog cilja pred inženjere iterativno postavlja nove zadatke koji se rezultuju novim rešenjima. Ta rešenja mogu biti jednostavne tehničke izmene nosećih protokola ili kompleksni inteligentni softverski sistemi koji uče i svoje odluke donose putem heurističkih metoda.

Greške koje se javljaju na računarskim mrežama i kod resursa koji su putem njih dostupni možemo podeliti u četiri kategorije na osnovu uzroka njihovog pojavljivanja:

1. Greške koje se pojavljuju usled propusta u definiciji hardverskih i softverskih komponenti računarskih mreža.
2. Greške koje se javljaju kao posledica neadekvatnog dizajniranja računarskih mreža i nenamenske upotrebe korišćenih komponenti.
3. Greške koje se javljaju usled neadekvatnog korišćenja računarskih mreža od strane korisnika nedovoljno obučениh za rad.
4. Greške koje se javljaju kao posledica iskorišćenja propusta u definiciji hardverskih/softverskih komponenti računarskih mreža, njihovom dizajnu i (ne)pažnji korisnika a od strane zlonamernih korisnika i u cilju ostvarivanja određene koristi od napada na računarsku mrežu ili resurs.

Iako greške svih pomenutih kategorija mogu imati katastrofalne posledice, ovo poglavlje se bavi greškama četvrtog tipa jer se one mogu klasifikovati kao napadi i sa sobom najčešće nose najveći negativan uticaj na poverljivost i dostupnost resursa i nesmetan rad mreže. Tema ovog poglavlja jeste bezbednost računarskih mreža ili tehnička rešenja za zaštitu računarskih mreža i putem njih dostupnih resursa od neregularnog korisničkog ponašanja.

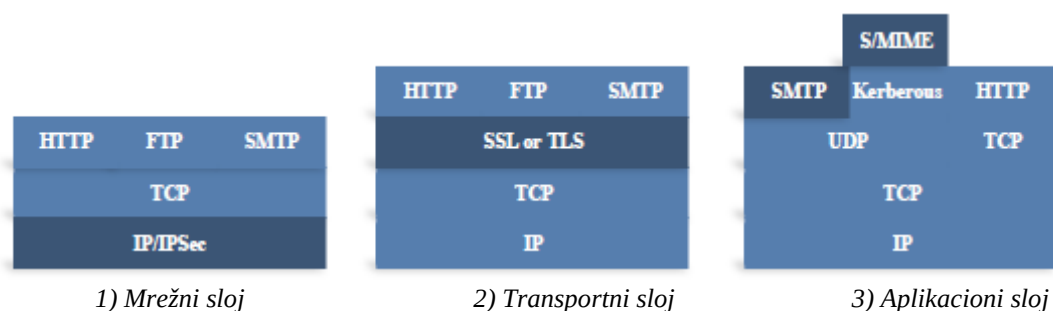
8.1. Bezbednost i zaštita servisa računarskih mreža

Skoro sve kompanije, većina vladinih agencija kao i mnogi pojedinci sada imaju svoje web sajtove. Broj pojedinaca kao i kompanija koji imaju pristup internetu se neverovatno povećava a svi oni imaju grafičke web pretraživače. Kao rezultat pomenutog, kompanije se raduju uspostavljanju mrežnih olakšica za elektronsko poslovanje. Ali činjenica je da su i internet i mreža jako podložni kompromitovanju raznih vrsta. Kako se kompanije suočavaju sa ovom realnošću, zahtevi za sve sigurnijim mrežnim uslugama rastu.

Svetska mreža zapravo predstavlja klijentsko-serversku aplikaciju koja funkcioniše putem interneta kao i TCP/IP mreža. S 'obzirom na to, bezbednosni alati i pristupi o kojima je bilo reči do sada jesu relevantni za pitanje mrežne sigurnosti. Mreža donosi nove izazove koji se u principu ne odobravaju mnogo u smislu kompjutera i mrežne sigurnosti.

8.2. Pristupi bezbednosti mrežnog saobraćaja

Postoji veliki broj pristupa za obezbeđenje mrežne sigurnosti. Ti isti razni pristupi su slični u smislu usluga koje pružaju i donekle u smislu mehanizama koje koriste, ali se razlikuju u smislu samog obima primenljivosti i relativnoj lokaciji u okviru TCP/IP protokola.



Slika 4. Relativna lokacija sigurnosti objekata u TCP/IP protokolima

Jedan od načina da se obezbedi mrežna sigurnost je da se koristi IP bezbednosni protokol (IPsec) (Slika a). Prednost Ipsec korišćenja je da je ista transparentna za krajnje korisnike i aplikacije, i pruža opšta rešenja. Šta više, Ipsec obuhvata i mogućnost filtriranja pa se tako samo odabrani saobraćaj ne izlaže Ipsec procesiranju.

Još jedno relativno opšte rešenje je da se primeni sigurnost odmah iznad linije kontrolnog protokola prenošenja (TCP – Transmission Control Protokol). Najistaknutiji primer ovakvog pristupa je sloj sigurnosnog adaptera (Secure Sockets Layer (SSL)) kao i

unapređeni internet standard poznatiji kao bezbednosni sloj prenosa (Transport Layer Security (TLS)). Na ovom nivou, postoje dva izbora implementacije. U velikoj većini slučajeva, SSL (ili TLS) mogu da se obezbede kao deo potpornog protokolnog programa pa bi stoga isti bili transparentni aplikacijama. Kao alternativa ovome, SSL može da se ugradi u posebne pakete. Na primer, Netscape, Microsoft Explorer, Mozilla Firefox, Google Chrome pretraživači već imaju u sebi ugrađen SSL, a većina veb servera ima već implementirani protokol.

Bezbednosne usluge koje su prilagođene određenim aplikacijama su već ugrađene u te određene aplikacije. Slika pod “c” predstavlja primer takve arhitekture. Prednost ovakvog pristupa je da usluga može da bude napravljena u skladu sa posebnim potrebama svake od datih aplikacija.

8.3. Zaštita na transportnom nivou

U vezi realizacije transportnih mehanizama zaštite, predlaže se primena standardnog SSL (Secure Sockets Layer) protokola (novija verzija je TLS (Transport Layer Security) protokol) između korisnika i web servera (ili web servisa).

U stvari, u informacionom sistemu organizacije predlaže se primena:

- SSL protokola sa serverskom autentikacijom – neophodan je SSL serverski sertifikat izdat za dati web server i
- SSL protokola sa klijentskom i serverskom autentikacijom na bazi digitalnih sertifikata i smart kartica korisnika. U ovom slučaju je takođe neophodno da web server (ili odgovarajući web servis) ima SSL serverski sertifikat.

Naime, za potrebe autentikacije korisnika informacionog sistema organizacije, predlaže se primena zaštite na transportnom nivou i jake autentikacije korisnika na bazi SSL protokola sa klijentskom i serverskom autentikacijom.

Dakle, u ovom slučaju nije samo dovoljno da web server poseduje sertifikat (serverska autentikacija) već je neophodno da u sistemu postoji, tj. koristi se i odgovarajuće Sertifikaciono telo (CA) koje izdaje sertifikate klijentima na smart karticama. Na ovaj način se postiže da samo klijenti sa smart karticama i odgovarajućim digitalnim sertifikatima mogu da pristupe datom web serveru, a samim tim da izvršavaju poslovne procese u okviru informacionog sistema organizacije.

Pomenuti mehanizmi zaštite na transportnom nivou predstavljaju SSL protokol sa klijentskom i serverskom autentikacijom. Svi navedeni tipovi korisnika imaju smart kartice na kojima je izgenerisan i smešten asimetrični privatni ključ i sertifikat.

Pri tome, korisnik se može autentikovati WEB serveru ili nekom web servisu a za autentikaciju može koristiti ili sam sertifikat (web aplikacije) ili thumbprint svog sertifikata, zajedno sa sertifikatom (web servis). U slučaju klijentske autentikacije na neki web servis sa kojim komunikacija podrazumeva prethodno uspostavljenu SSL sesiju sa uključenom klijentskom autentikacijom, tada sertifikat korisnika treba da, pored smart kartice, bude i na direktorijumu standalone softverske aplikacije koja služi za eventualni poziv web servisa ili se autentikacija sertifikata korisnika koji može da pristupi vrši na bazi thumbprint-a njegovog sertifikata. Šta će se koristiti za autentikaciju zavisi od konfiguracionog fajla u kome se nalazi zapisan način pozivanja datog web servisa.

Serverski SSL sertifikat treba da bude izgenerisan od strane odgovarajućeg CA tela sa dužinom ključa od 1024 ili 2048 bita. Takođe, treba primeniti default opciju za simetrični kriptografski algoritam: RC4 algoritam i dužinu ključa od 128 bita.

Mehanizme zaštite na aplikativnom nivou između korisnika i web/aplikativnog servera na bazi digitalnog potpisa i digitalne envelope na bazi smart kartica korisnika, moguće je realizovati na dva načina:

- Korisnik koristi web pretraživački (Internet browser) program (Internet Explorer), autentikuje se na bazi smart kartice i SSL klijentske autentikacije, a zatim koristi mehanizme zaštite na aplikativnom nivou za zaštitu fajlova ili html strana koje se dostavljaju do web/aplikativnog servera.
- Korisnik koristi klijentsku standalone aplikaciju (Windows aplikaciju) za čiji pristup se autentikuje na bazi smart kartice i izdatog digitalnog sertifikata. Komunikacija sa web serverom se realizuje putem web servisa koji se izvršavaju na web serveru. U klijentskoj aplikaciji se koristi digitalni potpis i digitalna envelope kao mehanizmi zaštite na aplikativnom nivou, kao i SSL protokol sa klijentskom autentikacijom između klijentske aplikacije i web servisa na strani web servera.

Što se tiče predloga primenjenih algoritama, kao i ranije predlaže se:

- Asimetrični privatni ključ korisnika – generisan na smart kartici i dužine 2048 bita.
- Asimetrični algoritam – RSA.
- Hash algoritam – najmanje SHA-1, ali i ostali pomenuti SHA algoritmi.
- Simetrični algoritam - 3DES ili AES sa dužinama ključeva 168 ili 128, 192 i 256 bita, respektivno.
- SSL serverski sertifikat – izdat od CA.
- Asimetrični par ključeva serverskog SSL sertifikata – 1024 bita.
- Simetrični algoritam u SSL protokolu – RC4 sa dužinom ključa 128 bita.

Svi dokumenti koji se razmenjuju u okviru informacionog sistema bi morali biti digitalno potpisani a samo pojedini (koji imaju odgovarajući stepen tajnosti) i šifrovani putem digitalne envelope.

Potrebno je zapaziti da se ovde radi i dvostrukom šifrovanju:

- primenom digitalne envelope na aplikativnom nivou
- u okviru SSL protokola na transportnom nivou.

To je neophodno iz razloga što se SSL šifrovanje terminira na web serveru koji je uobičajeno u DMZ zoni, dok se aplikativno šifrovanje (digitalna envelope) terminira na aplikativnom serveru koji je obično u internoj zoni. Pored toga, šifrovanje digitalnom envelopom je procedura šifrovanja za namenjenog primaoca (u ovom slučaju aplikativni server) i niko drugi tu poruku ne može da dešifruje.

Dakle, procedura zaštite u ovom slučaju bi se mogla realizovati tako što se prvo uspostavi SSL sesija sa web serverom na bazi klijentske autentikacije sa digitalnim sertifikatom klijenta na smart kartici, a zatim se u okviru klijentske aplikacije (ili Internet browser programa) vrši digitalni potpis i digitalna envelope poruka/fajlova koji se šalju kroz uspostavljeni SSL tunel i koje se procesiraju na aplikativnom serveru (u smislu dešifrovanja simetričnim kriptografskim algoritmom).

Za pomenute potrebe, neophodno je da i web i aplikativni server poseduju odgovarajuću krypto komponentu za realizaciju mehanizama aplikativne zaštite sa sledećim funkcijama:

- Kripto komponenta na web serveru – vrši verifikaciju digitalnog potpisa dostavljenih podataka i validaciju korisnikovog sertifikata. Ukoliko je pomenuta verifikacija/validacija uspešna, web server prosleđuje kompletne dostavljene podatke (sa digitalnim potpisom) do aplikativnog servera na odgovarajuće procesiranje i smeštanje u neku od baza organizacije.
- Kripto komponenta na aplikativnom serveru – vrši dešifrovanje podataka na aplikativnom nivou ukoliko je korisnik primenio postupak digitalne envelope za te podatke (podaci sa odgovarajućim stepenom tajnosti). Za tu svrhu, aplikativni server mora da ima, pored krypto komponente, i odgovarajuću smart karticu na kojoj je smešten privatni ključ kojim se dešifruju podaci (šifrovani korišćenjem odgovarajućeg digitalnog sertifikata) izdatog za aplikativni server. Podaci šifrovani primenom digitalne envelope se dešifruju na aplikativnom serveru i onda u otvorenom ili šifrovanom obliku čuvaju u bazi organizacije. To zavisi od stepena tajnosti datih podataka i predviđenog načina čuvanja podataka sa datim stepenom tajnosti. Što se tiče smart kartice i asimetričnih ključeva aplikativnog servera, važe isti zahtevi kao i za korisnike s jednom izmenom da je asimetrični ključ izgenerisan i bezbedno backup-ovan spolja (u CA) i upisan naknadno na smart karticu iz razloga disaster recovery procedure u slučaju kvara smart kartice.

S obzirom da se radi o SOA-baziranoj arhitekturi i da aplikativni slojevi (prezentacioni, aplikativni i data access) komuniciraju putem web servisa, za svaki od servera se generišu 2 SSL sertifikata (serverski i klijentski). Na taj način, između svaka dva servera u arhitekturi (web server – aplikativni server, aplikativni server – data access layer server) se uspostavlja SSL protokol sa klijentskom i serverskom autentikacijom.

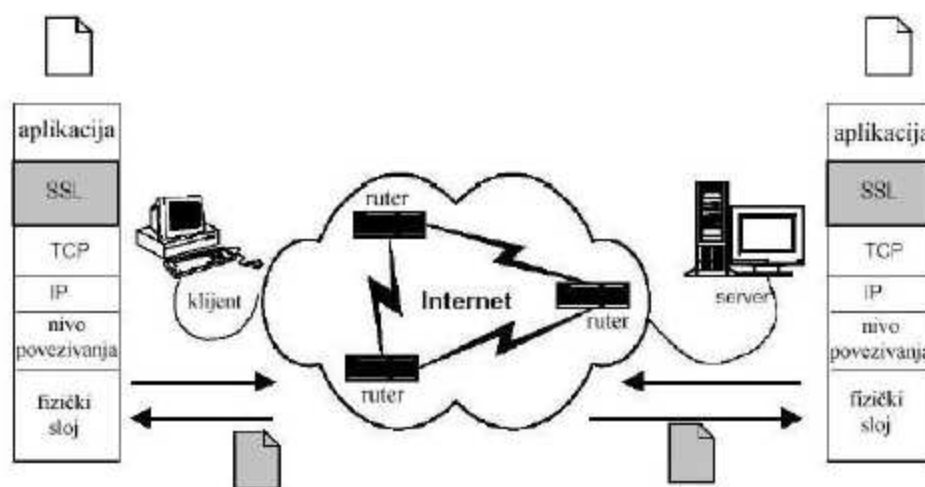
Time se podiže bezbednost čitavog sistema iz razloga što se tako vrši međusobna autentikacija između pomenutih servera a i čitava komunikacija je onda šifrovana kroz uspostavljene kriptografske tunele.

9. SSL protokol

Secure Sockets Layer (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 aplikacijski sloj. Od aplikacijskog 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, proveriti kontrolne brojeve, sastavi delove poruke, pa ih preda aplikacijskom 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 protokol je dizajniran i napravljen od Netscape Communications korporacije, da bi bio korišćen sa Netscape Navigatorom. Prva verzija, 1.0, je razvijena 1994.godine, međutim, to je bila samo probna verzija korišćena unutar ove korporacije. Verzija 2.0 je bila prva koja je izdata u javnost i koja je isporučivana sa Netscape Navigatorom, verzijama 1 i 2. Posle verzije SSL 2.0, Microsoft je izdao svoju verziju ovog protokola, koja je imala naziv PCT. Najnovija verzija SSL 3.0, je uključila sva poboljšanja Microsoftovog PCT-a, i time uklonila slabosti verzije SSL 2.0. U to vreme je, Internet Engineering Task Force (IETF) Transport Layer Security (TLS) grupa, koja je formirana 1996.godine, napravila otvoreni standard za šifrovanje zasnovan na SSL-u 3.0. Ovaj protokol je nazvan TLS verzija 1.0, i objavljen je 1999.godine na RFC 22461. Očekuje se da će TLS protokol biti standardizovan od strane IETF-a, i može se reći da se on razlikuje od SSL-a u nekoliko detalja. On je adaptiran od strane korisnika i projekatnata mobilnih radio uređaja, koji su prilagodili ovaj protokol bežičnim komunikacijama, i nazvali ga WTLS (Wireless TLS - bežični TLS).

SSL omogućava razmenu informacija između klijenta i servera, na transparentan način. Ovaj protokol je lociran između aplikacijskog i transportnog sloja ISO/OSI referencnog modela. Koristeći ovaj pristup, moguće je identifikovati SSL protokol kao deo sloja za prezentaciju. Na slici 5 se može videti mesto SSL-a u okviru TCP/IP protokola.

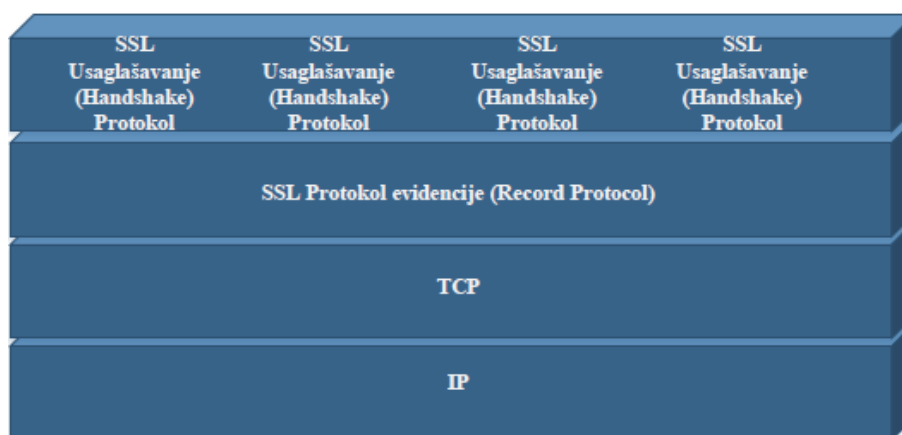


Slika 5: Funkcionalni model SSL protokola

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".

9.1. Arhitektura SSL-a

SSL je osmišljen da iskoristi TCP kako bi se uspostavila pouzdana bezbednosna usluga od početka do kraja. SSL ne predstavlja jedinstveni protokol već 2 sloja protokola, kao što je i predstavljeno na ilustraciji.



Slika 6. Slojevi SSL-a

SSL protokolna evidencija pruža osnovne bezbednosne usluge različitim protokolima koji se sastoje iz više slojeva. A posebno hipertext protokol prenosa (HTTP=Hypertext Transfer Protokol), koji pruža uslugu prenosa za interakciju web klijenta/servera, može funkcionisati povrh SSL. Tri protokola koja se sastoje iz više slojeva definišu se kao deo SSL: protokol sinhronizacije (usaglašavanje) (Handshake Protokol), specijalni protokol za promenu šifre (Change Cipher Spec Protokol), kao i protokol upozorenja (Alert Protokol).

Ovi SSL specifični protokoli se koriste za upravljanje SSL razmenom a biće opisani kasnije. Dva jako važna SSL koncepta su SSL sesija i SSL veza, koji su definisani u navedenim specifikacijama.

- Veza: veza predstavlja prenos (u definiciji slojevitog modela međuveze transporta otvorenog sistema (OSI)) koji pruža odgovarajući deo usluge. Za SSL, takve veze predstavljaju odnose klijent ka klijentu lokalne mreže. Veze su privremene a svaka veza se povezuje sa jednom od sesija.
- Sesija: SSL sesija predstavlja spoj između klijenta i servera. Sesije su stvorene Protokolom sinhronizacije. Sesije definišu set kriptografskih sigurnosnih parametara koje mogu da se dele među višestrukim vezama. Sesije se koriste kako bi se izbegla skupa pregovaranja oko novih sigurnosnih parametara za svaku vezu.

Između svakog para obe strane (aplikacije kao što su HTTP između klijenta i servera), mogu da postoje višestruke sigurnosne veze. U teoriji, takođe mogu da postoje višestruke simultane sesije između strana ali ova karakteristika se ne koristi u praksi.

Postoji nekoliko stanja koja se povezuju sa svakom od sesija. Jednom kada se sesija uspostavi, postoji trenutno operativno stanje i za čitaj i za piši (tačnije, primi i šalji). Pored toga, u toku Protokola sinhronizacije, stvaraju se čitaj i piši stanja na čekanju. Nakon uspešnog završetka Protokola sinhronizacije, ta stanja na čekanju postaju trenutna stanja.

Stanje sesije se definiše sledećim parametrima:

- Određivač sesija/Session identifier: proizvoljna bajt sekvenca odabrana od strane servera kako bi se identifikovalo aktivno ili obnovljivo stanje sesije.
- Sertifikat veze/Peer sertifikat: X509.v3 sertifikat klijenta. Ovaj element stanja može biti prazan/nepostojeći.
- Kompresivna metoda/Compression method: algoritam koji se koristi kako bi se kompresovali podaci pre šifrovanja.
- Specifikacija šifre/Cipher spec: određuje količinu podataka algoritma šifrovanja (kao što su nepostojeći, AES, itd.) i heš algoritma (kao što su MD5 ili SHA-1) koji se koriste za MAC računicu. Takođe definiše i kriptografska obeležja kao što je veličina heša.
- Glavna tajna/Master secret: 48-bajtovska tajna koja se deli između klijenta i servera.
- Obnovljivo je/Is resumable: zastavica koja ističe da li sesija može da se iskoristi da podstakne nove veze.

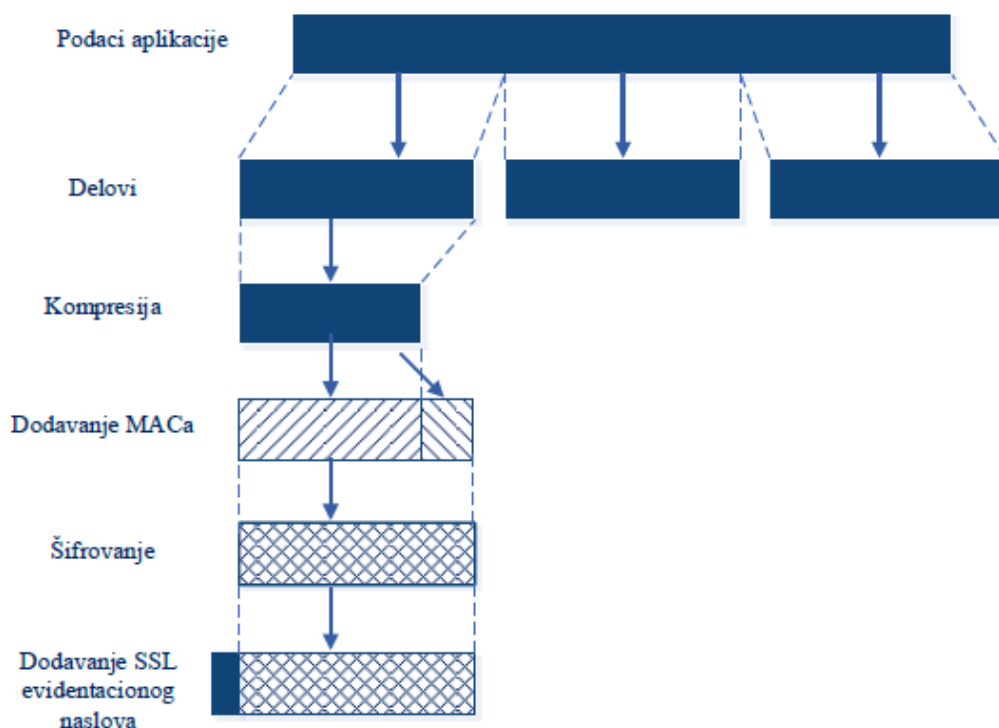
Stanje veze se definiše sledećim parametrima:

- Direktno server-klijent/Server and client random: bajt sekvence koje se biraju od strane servera i klijenta za svaku vezu.
- Serverski napisana MAC tajna/Server write MAC secret: tajni ključ koji se koristi u MAC operacijama za podatke koje šalje server.
- Klijentski napisana MAC tajna /Client write MAC secret: tajni ključ koji se koristi u MAC operacijama za podatke koje šalje klijent.
- Serverski napisan ključ/Server write key: tajni šifarski ključ za podatke enkriptovane od strane servera a koje dešifruje klijent.
- Klijentski napisan ključ/Client write key: simetričan šifarski ključ za podatke enkriptovane od strane klijenta a koje dešifruje server.
- Inicirajući vektori/Initialization vectors: kada se blok-šifra u CBC stanju upotrebi, inicirajući vektor (IV) se čuva za svaki ključ. Ovo polje je prvenstveno inicirano SSL Protokolom sinhronizacije. Nakon toga, krajnji blok šifrovani tekst iz svake evidencije se čuva za upotrebu kao IV sa sledećom evidencijom.
- Uzastopni brojevi/Sequence numbers: svaka strana čuva posebne uzastopne brojeve za slanje i primanje poruka svake od veza. Kada jedna od strana pošalje ili primi poruku za promenu specifikacije šifre, odgovarajući uzastopni broj dostiže nulu. Uzastopni brojevi ne smeju da premaše $2^{64} - 1$.

9.1.1. SSL protokol evidencije

SSL protokol evidencije (SSL Record Protocol) pruža dve usluge za SSL veze.

- Poverljivost: Protokol sinhronizacije definiše zajednički tajni ključ koji se koristi za klasično šifrovanje SSL paketa.
- Integritet poruke: Protokol sinhronizacije takođe definiše i zajednički tajni ključ koji se koristi kako bi se formirao kod autorizacije poruke (MAC).



Slika 7. Operacija dodavanja SSL zapisa

Ilustracija objašnjava celokupnu operaciju SSL protokola evidencije. Protokol evidencije preuzima aplikacionu poruku koja treba da se prenese, fragmentiše podatke u blokove kojima se može upravljati, opciono kompresuje podatke, primenjuje MAC, enkriptuje, dodaje zaglavlje i šalje dobijenu jedinicu u formi TCP segmenta. Primljeni podaci su dešifrovani, verifikovani, dekompresovani i ponovo sakupljeni pre nego što se isporuče ka višestrukim korisnicima.

Prvi korak je fragmentacija. Svaki gornji-sloj poruke se fragmentiše u blokove od 2^{14} bajta (16384 bajta) ili manje. Kao sledeće, opciono se primenjuje kompresovanje. Kompresovanje mora da bude bez gubitaka i ne sme da premaši dužinu sadržaja više od 1024 bajta. U SSLv3 (kao i trenutnoj verziji TLS-a), nijedan algoritam kompresije nije određen tako da je opšti kompresioni algoritam prazan/nepostojeći.

Sledeći korak je da se pristupi izračunavanju koda autorizacije poruke putem kompresovanih podataka. U ovu svrhu se koristi zajednički tajni ključ. Računica se definiše na sledeći način:

```
hash(MAC_write_secret || pad_2||
hash(MAC_write_secret || pad_1||seq_num ||
SSLCompressed.type || SSLCompressed.length ||
```

SSLCompressed.fragment))

Gde je:

|| Spajanje

MAC_write_secret

zajednički tajni ključ

hash

kriptografski heš algoritam; MD5 ili SHA - 1

pad_1

bajt 0k36 (0011 0110) ponavlja 48 puta (384 bita) za MD5 i 40 puta (320 bita) za SHA - 1

pad_2

bajt 0k5C (0101 1100) ponavlja 48 puta za MD5 i 40 puta za SHA - 1

seq_num

redni broj za ovu poruku

SSLCompressed.type

protokol višeg nivoa zadužen za obradu dela

SSLCompressed.length

dužina komprimovanog dela

SSLCompressed.fragment

kompresovani deo (ako se kompresija ne koristi , deo je otvorenom tekstu)

Treba istaći da je ovo jako slično HMAC algoritmu. Razlika je što su 2 potpore koncentrovane u SSLv3 a XOR-ovane u HMAC-u. SSLv3 MAC algoritam se zasniva na originalnom internet nacrtu za HMAC, koji koristi ulančavanje. Finalna verzija HMAC-a (definisana u RFC 2104) koristi XOR.

Kompresovana poruka plus MAC su enkriptovani uz pomoć simetričnog šifrovanja. Šifrovanje ne bi smelo da premaši dužinu sadržaja od 1024 bajta, tako da ukupna dužina ne sme da premaši $2^{14} + 2048$. Sledeći šifarski algoritmi se dozvoljavaju.

Tabela 1. Šifarski algoritmi dozvoljeni pri korišćenju SSLa

Blokovski šifrat		Šifrat niza	
Algoritam	Veličina ključa	Algoritam	Veličina ključa
AES	125, 256	RC4-40	40
IDEA	128	RC4-128	128
RC2-40	40		
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

Fortezza može da se upotrebi u šemi šifrovanja pametne kartice. Za redno šifrovanje, kompresovana poruka plus MAC se enkriptuju. Potrebno je istaći da se MAC računa pre nego što dođe do šifrovanja a onda se MAC šifrjuje zajedno sa nešifrovanim tekstom ili kompresovanim nešifrovanim tekstom.

Za blok šifrovanje, umetanje može da se doda nakon MAC-a, pre samog šifrovanja. Umetanje je u formi broja bajta umetanja praćeno jednobajtovskom indikacijom dužine umetanja. Celokupna količina umetanja predstavlja najmanju količinu, toliku da je ukupna

količina podataka koja treba da bude enkriptovana (nešifrovani tekst plus MAC plus umetanje) višestruka dužina bloka šifre. Primer je nešifrovani tekst (ili kompresovani tekst, ukoliko se kompresovanje koristi) od 58 bajta, sa MAC-om od 20 bajta (koji koriste SHA-1), koji je enkriptovan uz pomoć bloka dužine 8 bajta (npr, DES). Sa umetanjem dužine bajta, to daje total od 79 bajta. Kako bi se total načinio celobrojnim množiocem od 8, jedan bajt umetanja se dodaje.

Krajnji korak procesiranja SSL Protokola evidencije jeste priprema zaglavlja koje bi se sastojalo od sledećih polja:

- vrsta sadržaja (8 bita): višestruki protokol koji se koristi kako bi se procesirao priloženi fragment.
- jača verzija (8 bita): označava jaču verziju SSL u upotrebi. Za SSLv3, vrednost je 3.
- slabija verzija (8 bita): označava slabiju verziju u upotrebi. Za SSLv3, vrednost je 0.
- kompresovana dužina (16 bita): dužina bajta fragmenta nešifrovanog teksta (ili kompresovanog fragmenta, ukoliko se kompresovanje koristi). Maksimalna vrednost je $2^{14} + 2048$.



Slika 8. Format SSL zapisa

Vrste sadržaja koje su definisane su *change_cipher_spec*, *alert*, *handshake*, i *application_data*. Prve tri predstavljaju SSL-specifične protokole, i iste su sledeće o kojima će biti reči. Treba se istaći da se nikakva razlika ne pravi između raznih aplikacija (npr, HTTP) koje mogu da koriste SSL; sadržaj tih podataka stvoren takvom aplikacijom je nedokučiv za SSL. Slika 8. predstavlja SSL format evidencije.

9.1.2. Specijalni protokol za promenu šifrata

Specijalni protokol za promenu šifrata (Change Cipher Spec Protocol) predstavlja jedan od tri SSL-specifična protokola koji koristi SSL Protokol evidencije, i najjednostavniji je oblik protokola. Isti protokol se sastoji iz jedinstvene poruke (Slika 32a), koja se sastoji od pojedinačnog bajta sa vrednošću 1. Jedina svrha ove poruke je da izazove da se stanje na čekanju iskopira u trenutno stanje, što bi ažuriralo program šifrata da se iskoristi na ovoj vezi.



Slika 9. Paket SSL evidencionog zapisa

9.1.3. Protokol upozorenja

Protokol upozorenja (Alert Protocol) se koristi da se prenesu određene SSL uzbune na srodan entitet. A što se tiče ostalih aplikacija koje koriste SSL, poruke upozorenja se kompresuju i enkriptuju, kao što je i određeno trenutnim stanjem.

Svaka poruka u ovom protokolu se sastoji iz 2 bajta. Prvi bajt ima upozoravajuću vrednost (1) ili fatalnu (2) kako bi se prenela ozbiljnost poruke. Ukoliko se nivo pokaže fatalnim, SSL istog trenutka prekida vezu. Ostale veze na samoj sesiji se mogu nastaviti, ali se nove veze na istoj sesiji ne mogu uspostaviti. Drugi bajt sadrži kod koji ističe određeno upozorenje. Kao prvo, biće predstavljena ona upozorenja koja su uvek fatalna (definicije iz SSL specifikacija):

- *unexpected_poruka*: neprikladna poruka koja je primljena.
- *bad_record_mac*: neispravan MAC koji je primljen.
- *decompression_failure*: funkcija za dekompresiju koja je primila neispravne ulazne podatke (npr, nije u mogućnosti da dekompresuje ili da dekompresuje više od maksimalno dozvoljene dužine).
- *handshake_failure*: pošiljalac nije bio u mogućnosti da ispregovara prihvatljiv set sigurnosnih parametara, s'obzirom na dostupne mogućnosti.
- *illegal_parameter*: polje u poruci sinhronizacije je bilo van dometa ili nekonzistentno sa ostalim poljima.

Preostala upozorenja su sledeća:

- *close_notify*: obaveštava primaoca da pošiljalac neće slati više poruka sa te iste veze. Od svake strane se zahteva da pošalje *close_notify* upozorenje pre zatvaranja pismenog dela veze.
- *no_certificate*: može biti poslat kao odgovor na zahtev za sertifikatom ukoliko nijedan odgovarajući sertifikat nije dostupan.
- *bad_sertifikat*: primljeni sertifikat je nepravilan (npr, sadrži potpis koji nije verifikovan).
- *unsupported_sertifikat*: vrsta primljenog sertifikata koja nije podržana.
- *sertifikat_revoked*: sertifikat koji je opozvan od strane svog potpisnika.
- *sertifikat_expired*: sertifikat koji je istekao.
- *sertifikat_unknown*: neki drugi, neodređeni problem se pojavio u procesuiranju sertifikata, čineći ga neprihvatljivim

9.1.4. Protokol sinhronizacije

Najkompleksniji deo SSL-a je Protokol sinhronizacije. Ovaj protokol dozvoljava serveru i klijentu da autorizuju jedan drugog i da dogovore šifrovanje i MAC algoritam i kriptografske ključeve koji će se koristiti kako bi se zaštitili podaci poslani ka SSL evidenciji. Protokol sinhronizacije se koristi pre nego što se bilo koji aplikacioni podaci prenesu.

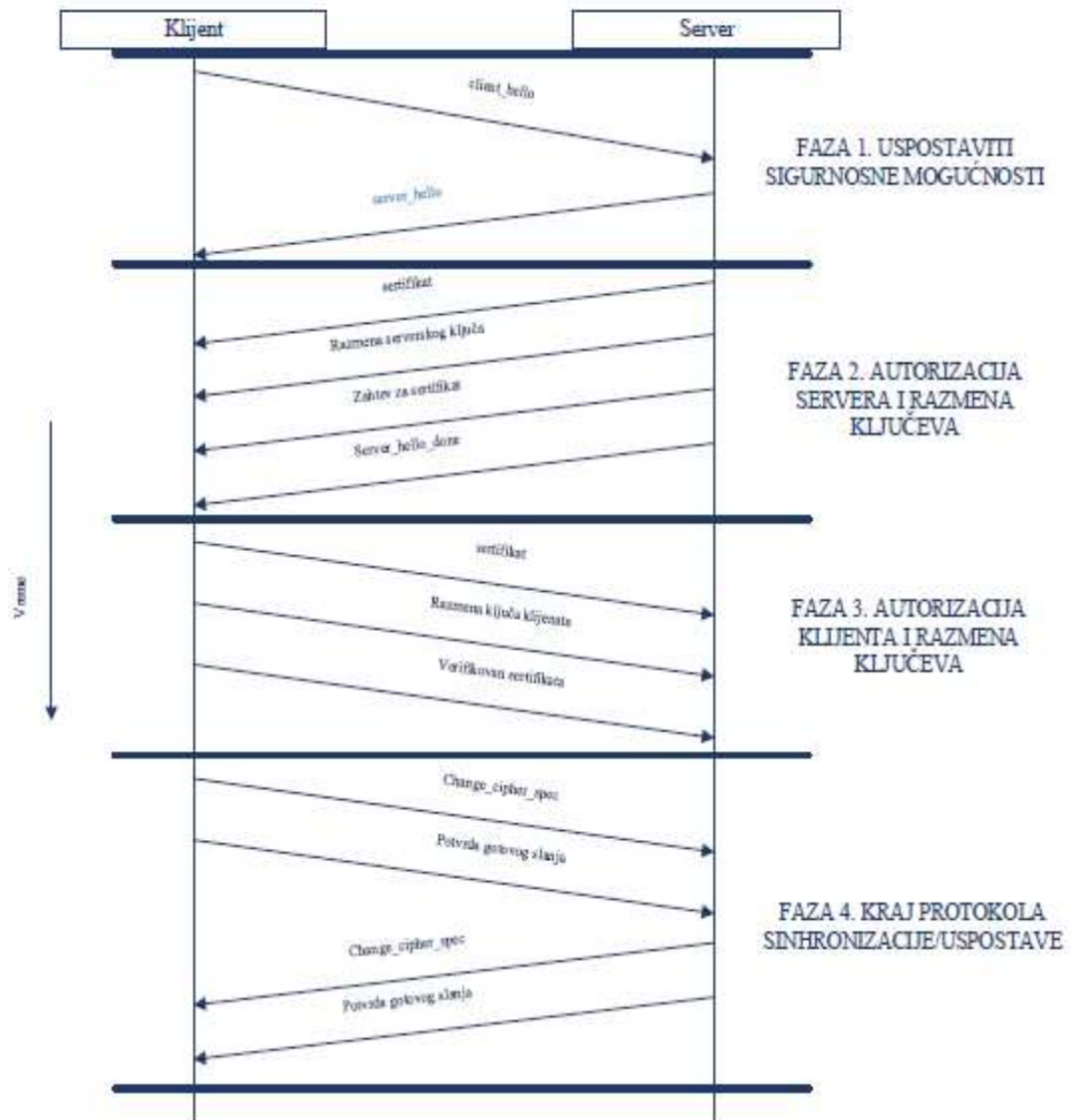
Protokol sinhronizacije se sastoji od serija poruka koje su razmenjene od strane klijenta i servera. Sve ove poruke imaju format kakva je predstavljen na ilustraciji Svaka od poruka ima 3 polja:

- vrsta (1 bajt): ističe jednu od 10 poruka. Tabela nabroja definisane vrste poruka.
- dužina (3 bajta): dužina poruke izražena u bajtovima.
- sadržaj (bajta): parametri koji se povezuju sa ovom porukom; isti su nabrojani u sledećoj tabeli.

Tabela 2. Parametri korišćeni u protokolu uspostave/sinhronizacije

Tip poruke	Parametri
hello_request	Null
client_hello	Verzija, ID sesije, metod kompresije, tip šifrata, slučajna vrednost
server_hello	Verzija, ID sesije, metod kompresije, tip šifrata, slučajna vrednost
Certificate	Ilanac sertifikata X.509v3
server_key_exchange	Parametri, potpis
certificate_request	Tip, ovlašćena tela
server_done	Null
certificate_verify	Potpis
client_key_exchang	Parametri, potpis
finished	Heš vrednost

Na slici je predstavljena inicijalna razmena koja je neophodna kako bi se uspostavila logična veza između klijenta i servera. Razmena može da se posmatra kroz 4 faze, koje su predstavljene na sledećoj slici.



Slika 10. Inicijalna razmena koja je neophodna kako bi se uspostavila veza između klijenta i servera

10. HTTPS

HTTPS (HTTP preko SSL) se odnosi na kombinaciju HTTP i SSL kako bi se implementirala sigurna komunikacija između veb pretraživača i mrežnog servera. Mogućnost postojanja HTTPS-a je ugrađena u sve moderne web pretraživače. Upotreba istog zavisi od web servera koji podržava HTTPS komunikaciju. Na primer, neki pretraživački uređaji ne podržavaju HTTPS.

Glavna razlika koja može da se vidi od strane korisnika web pretraživača jeste da URL (uniform resource locator – nepromenljiv detektor resursa) adrese počinju sa HTTPS:// a ne sa HTTP://. Normalna HTTP veza koristi port 80. Ukoliko je HTTPS određen, koristi se port 443, što „poziva“ SSL.

Kada se koristi HTTPS, sledeći elementi komunikacije se enkriptuju:

- URL zatraženog dokumenta
- sadržaj dokumenta
- sadržaj pretraživačkih formi (koje popunjava korisnik pretraživača)
- kolačići“ koji se šalju od pretraživača ka serveru i obrnuto
- sadržaj HTTP zaglavlja

HTTPS se dokumentuje u RFC 2818, HTTP preko TLS. Ne postoji neka značajna promena pri korišćenju HTTP-a putem SSL ili TLS-a, i obe primene se nazivaju HTTPS.

10.1. Iniciranje veze

Za HTTPS, činilac koji se ponaša kao HTTP klijent takođe predstavlja i TLS klijenta. Klijent inicira vezu ka serveru na odgovarajućem portu a onda šalje TLS ClientHello kako bi se započela TLS sinhronizacija. Kada se TLS sinhronizacija završi, klijent može onda da inicira prvi HTTP zahtev. Svi HTTP podaci se šalju kao TLS aplikacioni podaci. Normalno HTTP ponašanje, uključujući i zadržane veze, bi trebalo pratiti.

Potrebno je da se razjasni da postoje 3 nivoa svesnosti o vezi u HTTPS. Na HTTP nivou, HTTP klijent zahteva vezu na HTTP serveru time što šalje zahtev za vezu na sledeći najniži sloj. Obično je taj sledeći najniži sloj TCP, ali isti može takođe biti i TLS/SSL. Na TLS nivou, sesija se uspostavlja između TLS klijenta i TLS servera. Ova sesija može da podrži jednu ili više veza u bilo koje vreme. Kao što je već viđeno, TLS zahtev da se uspostavi veza počinje sa uspostavom TCP veze između TCP entiteta sa klijentove strane i TCP entiteta sa serverske strane.

10.2. Zatvaranje veze

HTTP klijent ili server mogu da istaknu zatvaranje veze time što će uključiti sledeći red u HTTP evidenciju: `connection: close`. Isto naglašava da će veza biti zatvorena nakon što se ova evidencija prenese.

Zatvaranje HTTPS veze zahteva da TLS zatvori vezu sa srodnim TLS entitetom daljinskim putem, što bi obuhvatilo zatvaranje potporne TCP veze. Na TLS nivou, pravilan način da se zatvori veza je da svaka strana upotrebi TLS protokol upozorenja kako bi poslala `close_notify` upozorenje. TLS implementacije moraju da iniciraju upozorenja pred zatvaranje pre zatvaranja same veze. TLS implementacija može i, nakon slanja upozorenja pred zatvaranje, zatvoriti samu vezu bez čekanja da druga strana pošalje svoje upozorenje pred zatvaranje, time stvarajući “nepotpuno zatvaranje”. Pažnja se treba obratiti da implementacija koja radi pomenuto može odabrati da ponovo upotrebi sesiju. Isto treba da se uradi samo u slučaju kada aplikacija zna (obično putem otkrivanja granica HTTP poruka) da su primljeni svi podaci poruke koji su joj od interesa.

HTTP klijenti moraju takođe znati da reaguju u situaciji kada se potporna TCP veza završava bez prethodnog `close_notify` upozorenja i bez `connection: close` indikatora. Do takve situacije može da dođe zbog programske greške na serveru ili komunikacione greške koja izazova da se TCP veza obustavi.

Međutim, nenajavljeno TCP zatvaranje može da bude i dokaz neke vrste napada. HTTPS klijent bi trebalo da izda neku vrstu bezbednosnog upozorenja svaki put kada se isto desi.

11. Slabosti SSL protokola

Rast i popularnost SSL aplikacija upućuje na opasnost od otkrivanja i iskorišćavanja sigurnosnih "rupa" u protokolu, koji bi mogli ugroziti sigurnost podataka koji se štite. Popularnost Interneta, i njegovih korisnika je u rastu svaki dan, i broj korisnika koji koriste elektronske transakcije raste isto tako. SSL je vrlo jeftin za implementaciju, i razvijen je kao brza solucija za potrebe sigurnosti u web aplikacijama, koje rade sa poverljivim podacima. To objašnjava više implementacija ovog protokola na Internetu. Međutim, kao i svaki drugim sistem, SSL nije u potpunosti siguran. SSL je dizajniran da osigura sledeće: poverljivost, integritet i proveru identiteta. Deo koji se odnosi na poverljivost je takav, da zlonamerna osoba može presresti osetljive informacije, u trenutku dok se šalju, ali se ti podaci ne mogu dešifrovati. Deo sa proverom identiteta je dizajniran da osujeti mogući "čovjek u sredini" napad, gde su poverljivi podaci preusmereni od strane zlonamerne osobe. Servis za proveru identiteta je dobro implementiran kroz potvrde, mada je moguće da postane žrtva napada.

11.1. Korisnička ubeđenja i pretpostavke

Jedan deo problema sigurnosti u vezi SSL-a, je preveliko poverenje koje korisnici imaju u ovaj protokol. Kako je korišćenje Interneta poraslo, i elektronska trgovina postala učestala u svakodnevnom životu ljudi, tako je razvijen i lažni osećaj sigurnosti. U ranoj fazi elektronskog poslovanja, ljudi su bili više skeptični u vezi sigurnosti na Internetu. Prosečni korisnik Interneta ne bih dao svoj broj kreditne kartice, ili neku drugu oseljivu informaciju preko Interneta. Ali sa povećanjem poslovanja pre Interneta, na kraju devedesetih, ljudi su postali samouvereni i sigurni, u svoje transakcije, od kupovine do plaćanja računa. Korisnik samo pogleda sličicu katanca u Internet Exploreru i već se oseća sigurnim. Ovo znači da je dosta poverenja razvijeno od strane korisnika:

- da SSL protokol nema mana;
- da je protokol ispravno ugrađen u Internet Explorer;
- i da je identifikacija potvrda u potpunosti proverena na sajtovima pre primene istih.

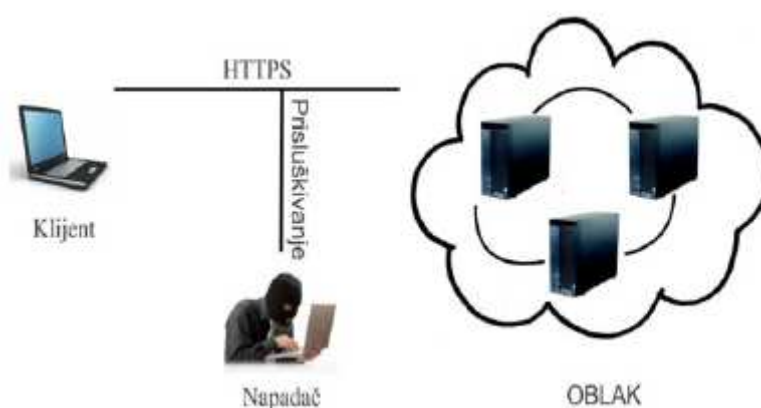
U drugim slučajevima, korisnici možda nemaju dovoljno znanje i osećaj za sigurnost poverljivih podataka. Na primer, ako se uzme za primer da zlonamerni web sajt koristi samopotpisane potvrde, tj. potvrde koje ovlašćena organizacija za identifikaciju potvrda nije odobrila. Kada browser pokuša da uspostavi SSL vezu, on će proveriti da li je potvrda koja je prisutna na serveru ispravna. Browser će utvrditi da potvrda nije potvrđena ni od jedne od poverljivih institucija za proveru potvrda, pa će postaviti pitanje korisniku da li želi da prihvati potvrdu koja nije potvrđena, i nastaviti proces povezivanja ako korisnik odgovori potvrdno. Međutim, u Internet Exploreru i Netscape-u, način na koji je prikazano obaveštenje ne objašnjava da postoji sigurnosni rizik za prihvatanje potvrda. Većina korisnika koja je suočena sa tom porukom, koju ne razume baš najbolje, će odgovoriti potvrdno sa "OK".

11.2. Lista organizacija za izdavanje potvrda

Jedna od glavnih mana implementacije SSL protokola je nedostatak adekvatne zaštite liste organizacija za overu i izdavanje potvrda, koju web browser smatra poverljivom i sigurnom. Ova lista može biti izmenjena od strane nekog opasnog virusa, kao što je crv, trojanac, ili neka druga vrsta napada. Zlonamerni kod može promeniti listu, i dodati SSL potvrdu u niz proverenih. Ova mana ugrožava komponentu za identifikaciju SSL-a, i pravi od komunikacije između klijenta i servera, potencijalnu žrtvu napada koja se naziva "čovjek u sredini".

11.3. Napad prisluškivanjem saobraćaja

Kako se inicijalni prenos podataka odvija u otvorenom tekstu pri SSL uspostavi veze, napadač može da dostavi podatke za ARP prevaru između klijenta i servera. Napadač presreće HTTPS zahtev od klijenta, i povezuje se sa samim serverom. Kada server pošalje sertifikat za autentifikaciju, napadač može da napravi sertifikat koji je sam potpisao, a zatim ga prosledi klijentu. Korisnici imaju tendenciju da izaberu prihvatanje lažnog sertifikata čak i ukoliko ih programski paketi upozoravaju na moguću prevaru. Ovo dodatno olakšava napad, pa napadač lako uspostavlja SSL komunikacioni link. Napad sadrži sledeće korake: lažiranje ARP saobraćaja omogućava umetanje napadača na relaciju server klijent. Tada napadač može da prati saobraćaj, tj. Pakete između klijenta i servera. Nakon ARP napada sledi DNS napad i prisluškivanje porta 443 preko koga se uspostavlja SSL saobraćaj. Kada napadač primeti SSL zahtev od strane klijenta, napadač tada prihvata TCP zahtev i inicira SSL vezu sa serverom. Nakon uspešne konekcije na server napadač sprema lažni sertifikat koji sam potpisuje i podmeće klijentu kako bi dalje mogao da dešifruje sav saobraćaj koji prisluškuje. Kada klijent primi lažni sertifikat, može se desiti situacija u kojoj će Internet pretraživač upozoriti da se radi o lažnom sertifikatu ili na mogućnost napada. Nakon prihvatanja lažnog sertifikata napad se smatra uspešnim jer i klijent i napadač šifruju sadržaj istim sertifikatom i imaju uspostavljenu SSL konekciju tako da se saobraćaj dalje može lako prisluškivati. Saobraćaj se može pratiti i pregledati u realnom vremenu.



Slika 11. Ilustracija prisluškivanja HTTPS saobraćaja

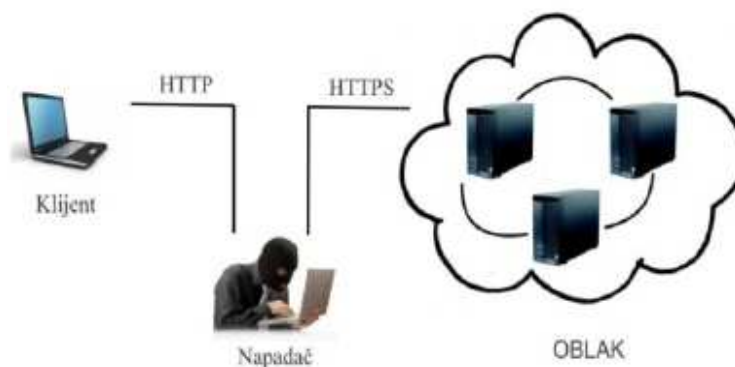
Danas postoji dosta specijalizovanih programa za ovu vrstu napada čija rešenja u sebe uključuju i ARP i DNS napad. Radi se o grafičkim rešenjima koja ne zahtevaju previše poznavanja računarskih mreža i protokola. Ova činjenica omogućava i slabije upućenim pojedincima da postanu napadači, ali omogućava i potencijalno veći broj žrtava. Većina

proizvođača Internet pretraživača se protiv ove vrste napada bori primarno detekcijom i sve upadljivijim upozorenjima koja od klijenata zahtevaju veću interakciju, osim do sada uobičajne interakcije od jednog klika.

11.4. Napad zaobilaženjem sigurne veze

Slično prvom napadu, napadač može da prosleđuje pakete i prati HTTP saobraćaj ARP varanjem između klijenta i servera. Kada napadač primeti da će saobraćaj sa običnog HTTP biti preusmeren na HTTPS saobraćaj, prosleđuje lažni saobraćaj klijentu. Sa druge strane, uspostavlja se lažna HTTPS veza sa serverom. Veza se uspostavlja sa lokacijom koju je klijent stvarno i želeo da poseti, a klijentu se prosleđuje sadržaj željene stranice kako ju je napadač primio, ali se stranica prosleđuje u HTTP obliku bez sertifikata i šifrovanja tako da je sadržaj dalje lako pratiti. Kako su podaci koji se razmenjuju sa klijentom u HTTP obliku i ne postoji provera sertifikata, nema načina da Internet pretraživači uoče bilo kakvu nepravilnost i upozore klijenta, tako da se u ovom napadu od klijente i ne zahteva nikakva interakcija. Samim tim uspešnost ovog napada je znatno izvesnija. Ovaj napada zahteva veće poznavanje sigurnosnih propusta i teže ga je implementirati. Napad je grafički predstavljen na sledećoj slici, i odvija se kroz sledeće korake:

- Sprovođenjem ARP napada napadač se umeće između servera i klijenta tako što i serveru i klijentu šalje lažne ARP pakete koji obmanjuju i klijenta i server.
- Napadač prati HTTP saobraćaj između servera i klijenta, prisluškujući i analizirajući saobraćaj.
- Napadač postaje aktivan tek kada primeti zahtev za HTTPS saobraćajem `<a href="https://...">`, nakon čega zahtev menja sa `<a href="http://...">`. Takođe se pravi lista svih adresa koje su zamenjene radi dalje lakše analize i manipulacije.
- Ukoliko napadač kasnije primi HTTP zahtev od klijenta na osnovu zapisa zna da treba da uspostavi HTTPS komunikaciju sa serverom.
- Nakon uspostavljanja HTTP zahteva sa klijentom, saobraćaj je otvoren (nezaštićen), a jedina manifestacija napada koju klijent može da primeti, ukoliko obrati pažnju, je sam zapis URL adrese u Internet pretraživaču. Pri normalno korišćenju sigurni saobraćaj bi u svojoj URL adresi sadržao https, dok će u slučaju napada u URL adresi sadržati samo http.



Slika 12. Preusmeravanje HTTP i HTTPS saobraćaja

11.5. Napad ubacivanjem potvrda

Ova vrsta napada je usmerena na ranjivost liste organizacija za izdavanje potvrda u Windowsu. Zlonamerna SSL potvrda može biti ubačena u browserovu listu poverljivih organizacija za proveru potvrda. Zbog toga je bitno ugraditi (updateovati) sve aplikacije na najnovije verzije koje su moguće, jer se tako uklanjaju sigurnosne "rupe" u programima. Postoji niz otkrivenih slabosti i propusta u Internet Exploreru i Windows Media Playeru, koje bi se mogle koristiti za ovu vrstu napada. Veličina ove pretnje je proporcionalna broju nezaštićenih i neobezbeđenih sistema, koji su još uvek ranjivi na ovu vrstu napada. U korporacijskim mrežama i serverima gde su sigurnosni sistemi pravilno održavani, opasnost je znatno manja. Međutim, kućni korisnici ne održavaju svoje računare u najsigurnijem stanju, pa su tako moguće velike izmene u njihovim sistemima. Drugi faktor koji omogućava ovu vrstu napada je operativni sistem. U korporacijskim mrežama moguće je koristiti datoteku i dozvole i registry bazu kroz listu pristupa za sprečavanje pristupa listi organizacija za proveru potvrda. Ali manje sigurni sistemi, kao što je Windows 98, nemaju takvu podršku. Kućni sistemi polako prelaze na verzije Windows 2000 i XP, ali i dalje postoji veliki broj korisnika prethodnih verzija ovog operativnog sistema. Ova mana je otkrivena tokom 2000. godine. Ona postoji u osnovnoj instalaciji različitih verzija operativnih sistema, kao što su: Windows 98, Windows NT Workstation, Windows 2000 Professional, i Windows XP Professional. Ovaj napad predstavlja preduslov za napad koji se naziva "čovjek u sredini".

11.6. Cipher suite - povratni napad

Jedan od glavnih propusta SSL protkola, odnosno njegove verzije 2.0, je cipher suite (niz parametara, kao što je algoritam za šifrovanje, itd.) povratni napad. Ovaj propust je ispravljen u verziji 3.0, ali još uvek postoji izvestan broj korisnika verzije 2.0. Ovaj napad se sastoji od toga da zlonamerna osoba neprimetno primorava korisnika da koristi slab algoritam za šifrovanje, iako postoje mnogo jači algoritmi. Ova vrsta napada se izvodi tako što se menja podržana lista cipher - suite parametara, koja se šalje tokom protokola povezivanja, i koja se šalje kao tekst kroz Hello poruku. Verzija 3.0 ovog protokola je rešila ovaj problem tako što obavlja identifikaciju svih poruka Handshake protokola kroz MasterSecret, tako da bi napadač mogao biti otkriven na kraju protokola i veza bi mogla biti prekinuta, ako je potrebno. Sve poruke Handshake protkola se šalju nešifrovane, ali umesto promene parametara koji se koriste, protokol razmene ključeva menja trenutno stranje veze. Pošto je povezivanje završeno, obe strane šalju poruku ChangeCipherSpec, koja obaveštava drugu stranu da izmeni svoje trenutno stanje veze na novo. Novo stanje veze se koristi od sledeće poruke. Posle ChangeCipherSpec poruke odmah se šalje Finished poruka, koja se sadrži MAC (kontrolni broj) na svim porukama Handshake protokola zaključanim od strane MasterSecreta. 48-bitni MasterSecret se nikad ne otkriva, umesto toga se ključevi veze generišu od njega. Finished poruka je zaštićena sa novo uspostavljenim parametrima veze (cipher suite). Ni jedna od strana u komunikaciji ne bi trebala prihvatiti podatke, sve dok se ne primi poruka Finished.

Tok poruka ide na sledećim redosledom:

1. $K \rightarrow S: [\text{ChangeCipherSpec}]$
2. $K \rightarrow S: [\text{Finished:}] \{a\}_k$
3. $S \rightarrow K: [\text{ChangeCipherSpec}]$
4. $S \rightarrow K: [\text{Finished:}] \{a\}_k$
5. $K \rightarrow S: \{m\}_k$

Gde $\{*\}_k$ predstavlja zaključanu šifrovanu transformaciju koju koristi Record sloj, m označava tekstualnu poruku koja se šalje pošto je razmena ključeva završena, dok a predstavlja identifikacioni kod Finished poruke, koji je dobijen izračunavanjem simetričnog MAC-a na prethodnim "handshake" porukama.

11.7. Problem male dužine ključeva

Sjedinjene Američke Države imaju dužu istoriju sprečavanja dužine ključeva za šifrovanje koji su namenjeni izvozu. Pre decembra 1998. godine, proizvodi za šifrovanje koji su izvoženi iz Sjedinjenih država nisu smeli imati više od 40-bitnog simetričnog ključa za šifrovanje, ili 512-bitnog asimetričnog. Istraživanjem velikog broja servera, došlo se do zaključka da 27% slabih servera podržava samo 40-bitni slabi niz parametara za šifrovanje. Browseri koji mogu da koriste samo 40-bitni nivo tih parametara će uspostaviti SSL vezu samo ako su ti parametri mogući i na serveru. Većina servera koji koriste slabe 40-bitne parametre zaštite će, takođe koristiti (512bitne) RSA ključeve. U istraživanju Erica Murraya (2000) se navodi da 83% SSL servera koristi isti nivo zaštite. Pošto ne treba mnogo da se "razbije" slabi RSA ključ, tada napadač može sav SSL saobraćaj prema serveru preuzeti.

11.8. Nedostatak HTTPS uspostave veze

Sadržaj podataka je otvoren pri SSL uspostavi veze, tako da napadač neovlašćenim pristupom i praćenjem može da dobije paket podataka. Kod SSL-a je moguć napad preuzimanja sesije. Klijent potvrđuje verodostojnost servera u koraku tri koji prenosi serverski sertifikat, ali sertifikat se prenosi u otvorenom tekstu i lako se može presretnuti i neovlašćeno koristiti. Kada napadač presretne poruku i dobije serverski sertifikat, može ga iskopirati i napraviti sopstveni lažni sertifikat, a zatim popuniti informacije sa podacima servera. Pri tom postavlja sopstveni javni ključ i potpis u sertifikat i dalje šalje falsifikovani sertifikat. Kada korisnici prihvate lažni sertifikat tada napad postaje uspešan. Dakle, postoji nedostatak u koraku tri pri SSL uspostavi veze.

Kao još jedna mana može se iskoristiti i samo poverenje korisnika u SSL i bezbednost sistema. Nakon brojnih analiza došlo se do zaključka da preko 95% korisnika ne obraća pažnju pri ukucavanju Web adrese i ne unosi samostalno HTTPS zahtev. Čak i kada korisnici koriste HTTPS zaštićeni pristup sajtu oni najčešće u svom pretraživaču ne unose adresu sa HTTP ili HTTPS delom, već jednostavno unose adresu u obliku: `www.sajt.com`. Svi Internet pretraživači će prvo pokušati da uspostave HTTP vezu kao pretpostavljeni tip veze. Tek nakon što se uspostavi veza sa serverom, serveri podešeni za sigurnu vezu će

poslati uputstvo sa redirekcijom na sigurni sajt u obliku `https://www.sajt.com`. Takođe čest je slučaj i da sam sajt u određenim delovima funkcioniše na osnovnom HTTP nivou bez zaštite (ukoliko se radi o prezentacionim materijalima koji ne zahtevaju interakciju korisnika), da bi tek nakon potrebe za interakcijom korisnika zahtevali sigurnu vezu za potrebu autentifikacije. Ovi slučajevi najčešće su rešeni postavljanjem istaknutih dugmića koji iniciraju sigurnu vezu. Većina saobraćaja funkcioniše preko običnog HTTP saobraćaja iz razloga što HTTPS saobraćaj dodatno opterećuje servere šifrovanjem informacij. Zavisno od slučaja do slučaja usporenja koja korisnik primećuje iznose od 2 do 100 puta. Iz ovog razloga sistemi su automatizovani pa samo bitni podaci koriste HTTPS saobraćaj. Zbog ovakvih i sličnih automatizovanih rešenja koja olakšavaju svakodnevno korišćenje Interneta i njegovih servisa sve manje korisnika obraća pažnju da li je uspostavljena obična HTTP ili sigurna HTTPS veza. Sa strane korisnika sve izgleda isto bez obzira na to da li je veza uspostavljena unosom cele adrese ili samo dela adrese. Sa strane mrežnog saobraćaja stvari ipak funkcionišu drugačije.

11.9. Uspostavljanje SSL veze

Na primeru klijent-server komunikacije prikazan je proces uspostavljanja SSL veze.



Slika 13. Uspostavljanje SSL veze

1. Klijent šalje ClientHello: Klijent šalje SSL pozdravnu poruku i pokazuje na početak uspostavljanja SSL veze. ClientHello poruka uključuje veličinu paketa, SSL verziju, slučajni broj koji generiše ključ klijenta, broj sesije, sve kriptografske pakete koji klijentski pretraživač može da podrži, metod kompresije koji može biti usvojen.

2. Server šalje ServerHello: Na primljenu ClientHello poruku poslatu od strane klijenta server odgovara sa porukom ServerHello. Poruka uključuje SSL verziju koju server najviše može da podrži, slučajni broj koji generiše server, broj sesije postavljen od strane servera, metode kompresije koje mogu biti usvojene.

3. Server šalje svoj sertifikat: Server šalje svoj autorizacioni lanac, koji uglavnom uključuje i sertifikat servera kao i viši sertifikat.

4. Server šalje ServerHelloDone: Server pokazuje da je sve autentifikacione informacije poslao klijentu u potpunosti.

5. Klijent šalje ClientKeyExchange: Nakon što klijent prođe proveru sertifikata koji je dobio od servera, klijent će generisati pre-master ključ, i korišćenjem javnog ključa sertifikata servera šifrovati pre-master ključ.

6. Klijent šalje ChangeCipherSpec: Klijent pokazuje da će sledeći mrežni paketi biti šifrovane od strane uspostavljenih ključeva za šifrovanje, a klijent generiše master ključ koji se koristi u komunikaciji kroz pre-master ključ i informacije koje su se razmenile ranije.

7. Klijent šalje Završeno: Klijent pokazuje da završava poruku u fazi uspostave veze.

8. Server šalje ChangeCipherSpec: Server pokazuje da će sledeća poruka biti šifrovana ključem koji je uspostavljen u toku kriptološke sinhronizacije.

9. Server šalje Završeno: Server pokazuje da je završio poruke u fazi potvrde uspostave veze.

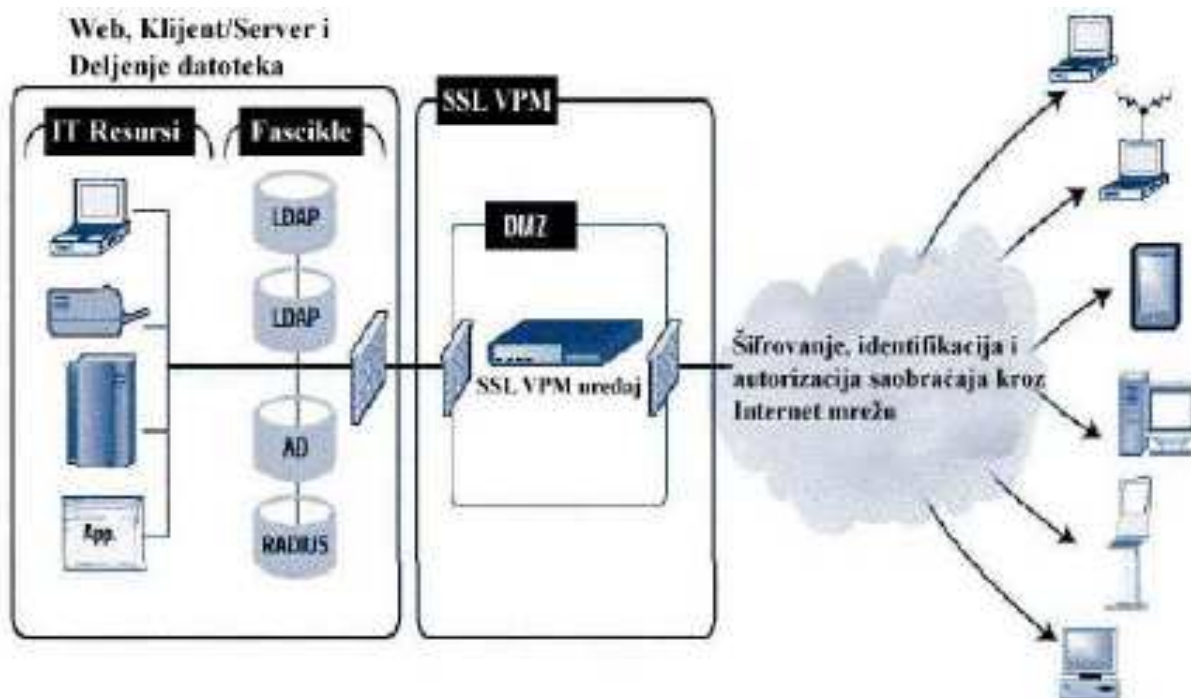
Nakon ovih koraka, komunikacija obe strane je šifrovana simetričnim šifarskim sistemom primenom uspostavljenog simetričnog tajnog ključa. Šifrovana komunikacija obezbeđuje sigurnost prenetih podataka između klijenta i servera.

12. SSL aplikacije

12.1. SSL bazirane virtuelne privatne mreže (VPM)

Virtuelne privatne mreže (VPM) koriste javnu telekomunikacionu infrastrukturu, kao što je Internet, da pruže razne usluge udaljenim kancelarijama i individualnim korisnicima. Kako se veze prenose preko provajdera Internet usluga, one pružaju određenu sigurnost i šifrovanje podataka. Dok je većina udaljenih pristupa danas implementirana koristeći IPsec, baziran na virtuelnim privatnim mrežama, veliki sistemi se sve više okreću SSL baziranim virtuelnim privatnim mrežama. Ovi servisi obično nude ograničen pristup kompanijskim resursima kroz standardne web browsere koristeći SSL. Jedan od glavnih razloga za ovaj trend je to što su SSL bazirane virtuelne privatne mreže lakše za instalaciju i upravljanje, i mogu da pruže pristup sa bilo kog mesta, zato što većina browsera podržava SSL.

SSL virtuelna privatna mreža koristi SSL i "proxije" (posredan pristup) da izvrši identifikaciju i siguran pristup za krajnjeg korisnika, za klijent/server, web i razmenu datoteka. Kada korisnik koji želi siguran pristup za privatnu mrežu, ukuca željenu adresu, on se automatski povezuje sa "proxy" (posredničkim) serverom koji stoji iza korporacijske mreže. Od te tačke, "proxy" server identifikuje korisnika, i pruža vezu između raznih aplikacijskih servera i udaljenih korisnika. Browser "misli" da komunicira direktno sa aplikacijom, a aplikacija misli da komunicira direktno sa browserom ili klijentskim programom.



Slika 14. SSL - VPM rešenje

Korišćenje posredničke tehnologije pruža kompaniji dodatnu sigurnost, zato što sprečava korisnika od pristupa sigurnoj mreži direktno, i omogućava korišćenje šireg spektra aplikacija koje SSL podržava. Sa SSL-om, svaka aplikacije je sigurna, za razliku od IPSec-a, koji se izvršava nezavisno od aplikacije. Pored toga, SSL se nalazi na višim slojevima protokola, i bliži je aplikacijskom sloju, što znači da pruža bolji kontrolni pristup koji omogućava pristup na daljinu i ekstranet, koji VPM zahteva. Kompanije mogu da odluče koji nivo sigurnosti žele, i koji ima najviše odgovara, a taj izbor uključuje:

- Identifikaciju korisničkog imena i šifre, ili X.509 digitalnu potvrdu;
- Šifrovanje 40-bitnim ili 128-bitnim RC4 ključem.

Prednosti korišćenja SSL - baziranih VPM-a:

- Lakše konfigurisanje i administriranje;
- Pruža pristup sa bilo kog mesta (uključujući javne kioske i PC-je);
- Niža cena;
- Posredni pristup pruža povećanu sigurnost.

Nedostaci SSL - baziranih VPM-a:

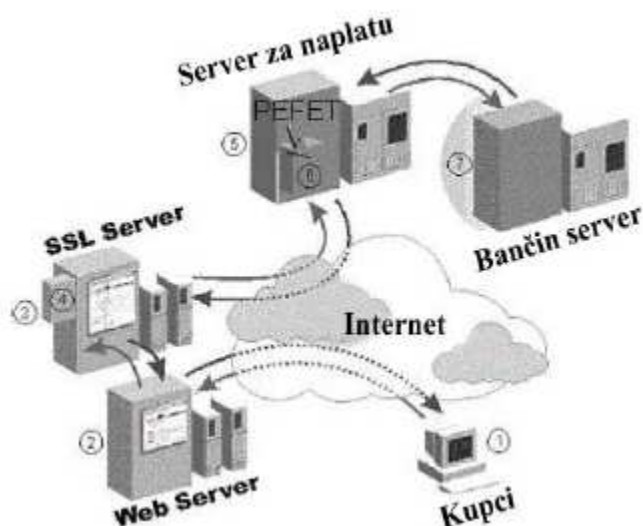
- Pristup je dozvoljen samo web aplikacijama;
- Osetljivost na napad "čovek u sredini";
- SSL pruža nedovoljnu proveru identiteta, u poređenju sa IPSec-om.

12.2. On-line plaćanje kreditnim karticama

Rast Interneta i World Wide Web-a je uticao na sve veću komercijalizaciju prodaje roba i usluga putem mreže. Danas, kreditne kartice predstavljaju osnovno sredstvo plaćanja za on-line kupovinu. Oko 90% on-line kupovina je učinjeno putem kreditne kartice. Na većini sajtova koji omogućavaju elektronsku trgovinu, za korisnike je najjednostavnije da kupe neki proizvod samo time što će ukucati broj kreditne kartice i dan isteka kartice. Postoje dva osnovna sigurnosna protokola za zaštitu on-line plaćanja: Secure Sockets Layer (SSL) i Secure Electronics Transaction (SET). SSL šalje šifrovane podatke direktno između korisnika i sajta na kojem se proizvod (usluga) kupuje.

Najnovije verzije poznatih web browsera, uključujući Netscape Communicator 7.1, omogućavaju korisnicima šifrovani prenos podataka u 128 -bitnom SSL razgovoru. Kada kupac poželi da kupi nešto na Internetu od prodavca koristeći SSL vezu, takav proces se može podeliti u dva koraka. U prvom koraku, dve strane uspostavljaju razgovor, a u drugom koraku se razmenjuju informacije između klijenta i servera kroz SSL vezu. Tada klijent

popunjava karticu za kupovinu i bira opciju za plaćanje. Uopšte, ovaj klijent mora uneti neke bitne lične informacije, kao što su broj kreditne kartice, dan isteka kartice, ime, i adresu. Sve te informacije na serveru se šifruju ponovo u SSL serveru, pa se onda šalje zahtev za naplatu kroz Internet. Na kraju se od banke traži provera identiteta. SSL server dobija ili dozvolu ili odbijanje za transakciju kroz server za plaćanje, i šalje rezultate kupcu i prodavcu. Sigurnost ovakvog načina plaćanja se može videti na sledećoj slici.



Slika 15. Sigurnost plaćanja kreditnom karticom preko Interneta

1. Kupac;
2. Server za e-poslovanje;
3. SSL server koji sadrži stranicu sa uplatom;
4. Administrativni alati koje koristi prodavac;
5. Server za naplatu (plaćanja);
6. Podsystem za prevare;
7. Server banke.

Ovakve transakcije moraju da se procesiraju na siguran način, tako da informacije o plaćanje ne mogu biti izmenjene tokom prenosa. Međutim, korisnik želi da bude siguran da su informacije o njegovoj kreditnoj kartici sigurne. Prodavac želi da bude siguran da će plaćanje biti obavljeno bez ometanja. Koristeći SSL vezu, pružena je odgovarajuća sigurnost za zaštitu od ovakvih rizika, pre svega što SSL pruža šifrovanje podataka, identifikaciju servera, integritet poruke, i opcionalnu identifikaciju klijenta preko TCP/IP protokola.

12.3. S-HTTP i SSL

Sigurni hiper - tekst transfer protokol (S-HTTP) je sigurnosni podsistem HTTP-a, i razvijen je od Enterprise Integration Technologies kompanije. Oba, S-HTTP i SSL pružaju mogućnost sigurne komunikacije sa web serverima, i oba se mogu koristiti da bi se obezbedila poverljivost, identifikacija, i integritet (nepromenljivost) podataka. Međutim, ovi pristupi se razlikuju u sledećim elementima:

SSL šifruje celu Internet vezu na nižem sloju, između aplikacijskih protokola, kao što su HTTP i TCP/IP slojevi. Ali S-HTTP radi na istom sloju kao HTTP. On osigurava razgovor obuhvatajući podatke unutar sigurnosnog paketa.

- SSL koristi specijalni "handshake" da bi uspostavio parametre za sigurnu vezu. S-HTTP definiše sigurnost razmenom zaglavlja za pakete poslate tokom web razgovora. Ova razmena zaglavlja paketa se može definisati kao vrsta sigurnih tehnologija koje se koriste u vezi.

- S-HTTP podržava širok spektar opcija za obezbeđivanje sigurnih parametara. Opcije koje podržava prave od S-HTTP-a fleksibilan sistem, ali i sistem koji je vrlo težak za konfigurisanje na web sajtu. SSL takođe pruža veliki broj opcija koji garantuju sigurnosne parametre, i ove opcije su pre - konfigurisane u browseru i serverima, što čini da SSL bude lakši za korišćenje.

- Ove mogućnosti današnjih web browsera pružaju mogućnost SSL-u da bude dominantna tehnologija za sigurne web veze. Kao rezultat toga, on-line plaćanja kreditnim karticama se većinom izvode uz pomoć SSL veza.

13. Predložena rešenja za SSL protokol

Zbog rastućih zahteva na polju bezbednosti i sigurnosti na Internetu, nastao je SSL protokol. Kompanija Netscape Communications se u pravo vreme našla na tržištu, kao stvaraoc ovog protokola, i zbog jake uloge na tržištu web browser-a, pa je isti postao veoma zastupljen.

SSL, osim što je odobren kao standard od strane WWW konzorcijuma (www.w3.org) postao je de facto standardom. Uz SSL razvijala su se i druga rešenja koja ostvaruju zaštićeni prenos podataka kroz mrežu. Uspešnost SSL-a dodatno je naglašena nedostatkom drugih dovoljno dobrih rešenja koji bi ga zamenili. Ovde su dati kraći pregledi nekih od rešenja.

S-MIME

Secure-MIME protokol je razvila RSA i dodatak je već postojećem MIME protokolu. Koristi sistem javnih ključeva kao osnovu za proveru ispravnosti i šifrovanje. Algoritmi za šifrovanje i rad sa potvrdama identični su onima korišćenim u SSL-u, tako da se iste potvrde mogu koristiti i u ovom protokolu. Korisnicima MIME-a, SMIME omogućava zaštitu identičnu u ovom radu opisanoj zaštiti koju pruža SSL.

S-HTTP

Secure HTTP je dodatak HTTP-u, on deluje u aplikacijskom sloju ISO/OSI modela. Za razliku od SSL-a koji ima zadatak da ostvari zaštićeni kanal između klijenta i servera, S-HTTP ima za cilj zaštićeno preneti pojedinačnu poruku. Takođe, omogućava proveru ispravnosti pošiljaoca poruke, te šifrovanje poruke kao i SSL. Razlog nerasprostranjenosti ovog protokola je neuspešan marketing koji ga je pratio, iako zadovoljava većinu zahteva traženih na tržištu.

SSH

Secure Shell se koristi za spajanje na udaljeni računar. Stvara zaštićeni kanal između dva računara, a identifikacija se vrši pomoću lozinke, koju pre slanja kroz mrežu šifruje. Ne omogućava identifikaciju pomoću potvrda.

PEM

Private Enhanced Mail omogućava zaštićeni prenos e-mail poruka koristeći proveru ispravnosti potvrdama, zaštitu sistemom javnih ključeva i proveru integriteta pomoću kontrolnog broja. PEM nije vezan za neki određeni operativni sistem ili vrstu korisnika, pa ga podržava veliki broj softverskih proizvoda. Ograničenje koje postavlja PEM je mogućnost slanja samo tekstualnih poruka.

PCT

Private Communication Technology je proizvod Microsofta koji je nastao kao reakcija na SSL verziju 2. Ta verzija SSL-a je imala probleme u situacijama kada je došlo do nasilnog prekida veze, čime je napadač dobio priliku da se uključi u razgovor bez identifikacije.

14. Zaključak

Problem bezbednosti u žičnim i bežičnim računarskim mrežama svakako postoji. Cilj ovog rada je upućivanje šireg auditorijuma u postojanje problema. Kroz rad je prikazano da i u najpouzdanijim metodama koje se koriste u najvećim sistemima, za koje većina smatra da su bezbedni, postoje mana koje zlonamerni korisnici mogu iskoristiti. Od situacije u kojoj su napade sprovodili retki izuzetno upućeni i teorijski dobro potkovani pojedinci, došlo se do situacije da današnji alati za penetracijske testove ne zahtevaju previše znanja od korisnika. Ovakve alate koji su prevashodno napravljeni za penetracijsko testiranje i dijagnostikovanje računarskih mreža zlonamerni pojedinci koriste u cilju dobijanja lične koristi. Zbog svega navedenog autori rada smatraju bitnom tematiku bezbednosti i podizanje svesti o propustima koji mogu biti zlonamerno iskorišćeni.

Nivo zaštite podataka kod razmene elektronskih poruka izuzetno je značajan element na osnovu kojeg se korisnici opredeljuju za ili protiv primene e-transakcija. To je posebno karakteristično u slučajevima kada gubitak, izmena, neovlašćeni uvid ili neke druge pretnje elektronskim dokumentima mogu da izazovu značajne pravne i finansijske posledice po učesniku u on-line transakciji. Naime, u e-poslovanju i razmeni elektronskih dokumenata učestvuju brojni partneri i svi moraju da imaju odgovarajući nivo zaštite.

Sa brzim razvojem mrežnih aplikacija, problem bezbednog prenosa postaje veoma važan. Zbog toga je SSL (Secure Sockets Layer) protokol sve više u širokoj upotrebi u različitim mrežnim servisima. Ovaj protokol sam po sebi nije savršen i u praksi sa njim često postoje problemi.

Danas u savremenom poslovanju, dosta autora predlaže sopstvena rešenja. Postoji nekoliko protivmera koje sprečavaju napade na SSL/TLS (Secure Sockets Layer / Transport Layer Security), bazirane na aplikaciji za internet poslovanje, e-trgovinu i e-bankarstvo. Većina autora predlaže rešenja u kojima je važno shvatiti da SSL/TLS protokol može zaštititi od napada, ali samo ako korisnik i server poseduju važeće sertifikate i ako se istovremeno identifikuju koristeći ove sertifikate.

Elektronsko poslovanje nesporno je donelo mnoge „blagodeti“, ali i brojne opasnosti. Što je njegov rast i zastupljenost veća, to su i posledice zloupotrebe teže. U zemljama u kojima se ovaj oblik poslovanja nalazi u stalnoj ekspanziji, preduzimaju se mnogobrojne aktivnosti u zaštiti, ali i hvatanju i kažnjavanju onih kojima zloupotrebe postaju „zanimanje“.

Literatura

- [1] Michael Howard, "Man-in-the-Middle Attack to the HTTPS Protocol", IEEE computer society, 2009, p.78-81.
- [2] S.Thomas. SSL and TLS Essentials. New york: Wiley Computing Publishing, 2004.
- [3] Moxie, Sslstrip. <http://www.thoughtcrime.org/software/sslstrip/>
- [4] T.Dierks and C.Allen, The TLS Protocol, IETF RFC 2246, 1999; www.ietf.org/rfc/rfc2246.txt.
- [5] Ponemon Institute© Research Report, Cost of Cyber Crime Study, August 2011
- [6] Analysis of the wireless network security IEEE 802.11 - The city of Belgrade, Saša Adamović Marko Šarac, Dalibor Radovanović, Infotech Jahorina, 2011/3
- [7] Certified Wireless Analysis Professional Official Study Guide (Exam PW0-205) bPlanet3 Wireless (Paperback - Oct 15, 2004)
- [8] 802.11 Wireless Networks: Security and Analysis (Computer Communications and Networks) by Alan Holt and Chi-Yu Huang (Hardcover - Jul 8, 2010)
- [9] Wikipedia, Information Security, http://en.wikipedia.org/wiki/Information_security
- [10] Joseph Steinberg and Tim Speed, Understanding SSL VPN, Packt Publishing, 2005.
- [11] Grupa autora, Guide to SSL VPNs, National Institute of Standards and Technology, 2008.
- [12] Spec.App Željko Pekić, SSL bezbjednost transportnog sloja, Univerzitet Mediteran, 2009.
- [13] Wikipedia, Information Security, http://en.wikipedia.org/wiki/Information_security
- [14] Wikipedia, Kriptozaštita, <http://sr.wikipedia.org/wiki>
- [15] Wikipedia, OSI model, , <http://sr.wikipedia.org/wiki>
- [16] Wikipedia, Virtualna privatna mreža, <http://sr.wikipedia.org/wiki>
- [17] Joseph Steinberg and Tim Speed, Understanding SSL VPN, Packt Publishing, 2005.
- [18] Grupa autora, Guide to SSL VPNs, National Institute of Standards and Technology, 2008.
- [19] Spec.App Željko Pekić, SSL bezbjednost transportnog sloja, Univerzitet Mediteran, 2009.
- [20] Verica Vasiljević, Računarske mreže, VŠER, 2008.
- [21] Zakon o elektronskom potpisu RS
- [22] Organizacija zaštite savremenih informacionih sistema, Bojan Ikić, Univerzitet Singidunum, 2011.