Secure Sockets Layer - SSL
Vrsta: Seminarski | Broj strana: 21 | Nivo: Fakultet za informatiku i menadžment

SADRŽAJ

1. Funkcionalni opis protokola

1.1. Opšti prikaz SSL protokola

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, proveri kontrolne brojeve, sastavi delove poruke, pa ih preda aplikacijskom sloju. Na taj naĉin se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mreţu. Ukoliko su klijent i server neaktivni duţe 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 Nescape Navigatorom. Prva verzija, 1.0, je razvijena 1994. godine, meĈutim, to je bila samo probna verzija korišćena unutar ove korporacije. Verzija 2.0 je bila prva koja je izdata u javnost i koja je isporuĉivana 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 ukljuĉila 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. Oćekuje se da će TLS protokol biti standardizovan od strane IETF-a, i moţe se reći da se on razlikuje od SSL-a u nekoliko detalja. On je adaptiran od strane korisnika i projektanata mobilnih radio ureĆaja, koji su prilagodili ovaj protokol beţiĉnim komunikacijama, i nazvali ga WTLS (Wireless TLS - beţiĉni TLS). SSL omogućava razmenu informacija izmeĆu klijenta i servera, na transparentan naĉin. Ovaj protokol je lociran izmeĆu aplikacijskog i transportnog sloja ISO/OSI referencnog modela. Koristeći ovaj pristup, moguće je identifikovati SSL protokol kao deo sloja za prezentaciju. Na slici 1 se moţe videti mesto SSL-a u okviru TCP/IP protokola.