

SADRŽAJ

1. FUNKCIONALNI OPIS PROTOKOLA	
3 1.1. OPŠTI PRIKAZ SSL PROTOKOLA	
.....	3 1.2. GENERISANJE
KLJUČA.....	5 1.3. SSL
HANDSHAKE PROTOKOL.....	6
1.4. SSL CHANGECIPHERSPEC PROTOKOL	
.....	8 1.5. SSL RECORD PROTOKOL
.....	8 1.6. SSL ALERT
PROTOKOL	10 2.
SLABOSTI I RANJIVOSTI SSL PROTOKOLA	11
2.1. KORISNIČKA UBEĐENJA I PRETPOSTAVKE	
.....	11 2.2. LISTA ORGANIZACIJA ZA
IZDAVANJE POTVRDA	12 2.3. NAPAD
UBACIVANJEM POTVRDA	12 2.4.
NAPAD "ČOVEK U SREDINI"	
12 2.5. CIPHER SUITE - POVRATNI NAPAD	
.....	13 2.6. PROBLEM MALE DUŽINE
KLJUČEVA	14 3. APLIKACIJE ZA
SSL	15 3.1. SSL
BAZIRANE VIRTUELNE PRIVATNE MREŽE (VPM)	
15 3.2. ON-LINE PLAĆANJE KREDITNIM KARTICAMA	
.....	16 3.3. S-HTTP I SSL
.....	17 4. SSL
PROTOKOL U PRIMENI	19 5.
LITERATURA	

21

2

Secure Sockets Layer - SSL

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, šifrjuje, eventualno kompresuje, a zatim te delove pošalje. Primalac primi delove, dekompresuje, dešifrjuje, 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 projektanata 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 1 se može videti mesto SSL-a u okviru TCP/IP protokola.

**----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE
PREUZETI NA SAJTU. -----**

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com