HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Secure Socket Layer

CCERT-PUBDOC-2000-07-01

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. OPIS 4

2.1. SLOJ ZAPISA 4
2.2. PROTOKOL ZA IZVANREDNE DOGAĐAJE (*ALERT*) 5
2.3. PROTOKOL ZA PROMJENU NAČINA ŠIFRIRANJA (*CHANGECIPHERSPEC*) 6
2.4. PROTOKOL ZA RUKOVANJE (*HANDSHAKE*) 6
2.4.1. ClientHello 6
2.4.2. ServerHello 7
2.4.3. Poslužiteljsko uvjerenje 7
2.4.4. ServerKeyExchange 7
2.4.5. CertificateRequest 7
2.4.6. Klijentsko uvjerenje 8
2.4.7. ClientKeyExchange 8
2.4.8. CertificateVerify 8
2.4.9. ChangeCipherSpec 9
2.4.10. Završna poruka 9

1. Uvod

SSL 3.0 protokol sastoji se od dva sloja:

- sloj poruka (korisničke poruke, poruke za rukovanje, poruke o izvanrednim događajima, poruke o promjeni načina šifriranja),
- sloj zapisa (SSL zapisi).
- Ova dva sloja nalaze se povrh prijenosnog sloja (obično TCP/IP). Isto tako SSL 3.0 definira i tri vrste poruka (protokola):
- protokol za izvanredne događaje (*engl. Alert protocol*)
- protokol za promjenu načina šifriranja (*engl. ChangeCipherSpec protocol*)
- protokol za rukovanje (*engl. Handshake protocol*)

SSL protokoli predstavljaju specijalne poruke koje se šalju korištenjem sloja zapisa. Sloj zapisa također služi za slanje korisničkih podataka.

2. Opis

2.1. Sloj zapisa

Sloj zapisa zadužen je za slanje blokova podataka (zapisa) između klijenta i poslužitelja. Veličina blokova je promjenjiva i može biti maksimalno 16 383 okteta. Prema specifikaciji u tom sloju granice poruka nisu očuvane. U načelu to znači da ukoliko proces iz višeg sloja brzo šalje poruke one se unutar sloja zapisa mogu grupirati u jedan zapis. Isto tako jedna poruka može biti podijeljena u više zapisa.
Svaki SSL zapis sadrži sljedeće informacije:

- tip sadržaja (engl. content type),
- verziju protokola,
- duljinu,
- podatke (opcionalno komprimirane i šifrirane),
- autentikacijski kôd poruke (engl. message authentication code – MAC).

Svaki zapis se komprimira i šifrira sukladno važećim algoritmima za šifriranje i komprimiranje. Na početku svake veze odgovarajuće vrijednosti za algoritme postavljaju se tako da inicijalno nema kompresije niti šifriranja.
MAC se određuje korištenjem formule:

```
hash(MAC_write_secret + pad2 +
      hash(MAC_write_secret  +  pad1  +  seq_number  +  length  +
content))
```

Elementi formule opisani su u tablici C-1.
SSL V3.0 također definira tri protokola

- protokol za izvanredne događaje (*engl. alert protocol*)
- protokol za promjenu načina šifriranja (*engl. ChangeCipherSpec protocol*)
- protokol za rukovanje (*engl. Handshake protocol*)

SSL protokoli predstavljaju specijalne poruke koje se šalju korištenjem sloja zapisa. Sloj zapisa također služi za slanje korisničkih podataka.

Polje	Opis
MAC_write_secret	je glavni tajni ključ koji SSL poslužitelj i klijent dijele
pad1	Niz ASCII znakova 0x36 ponovljen 48 puta za MD51, 40 puta za SHA-12. Sadržaj ovog polja je proizvoljan i koristi se da bi izračun MAC kôda bio što sigurniji.

[1] Message Digest v5; jednosmjerna funkcija podržana SSL 3.0 standardom

[2] Secure Hash Algorithm; jednosmjerna funkcija podržana SSL 3.0 standardom

Polje	Opis
pad2	Niz ASCII znakova 0x5C ponovljen 48 puta za MD5, 40 puta za SHA-1. Sadržaj ovog polja je također proizvoljan.
seq_num	Ovo polje predstavlja jedinstveni sekvencijski broj poruke.
hash()	Algoritam jednosmjerne funkcije koji je specificiran u trenutnom načinu šifriranja.

Tablica 1: *Polja Autentikacijskog kôda poruke*

2.2. Protokol za izvanredne događaje (*Alert*)

Izvanredni događaji jesu specijalne poruke koje se mogu poslati korištenjem sloja zapisa. Poruke o izvanrednom događaju sastoji se od dva dijela: razine (*engl. AlertLevel*) i opisa (*engl. Alert description*). Jedan i drugi dio kôdirani su kao 8-bitni brojevi (oktet).
SSL izvanredni događaji se šifriraju i komprimiraju. Standard definira dvije razine koje su opisani u tablici 3. Standard također definira 13 različitih opisa izvanrednih događaja koji su opisani u tablici 2.

Broj	Ime	Opis
0	close_notify	Indicira da pošiljatelj više ne kani slati podatke. Ukoliko je ovaj opis poslan sa upozorenjem, sjednica može biti obnovljena; ukoliko je pak poslan uz fatalnu razinu događaja, sjednica na može biti obnovljena.
10	unexpected_message	Primljena je neočekivana poruka. Ovaj opis se ne bi smio dogoditi; indicira pogrešku u jednoj od SSL implementacija (klijentskoj ili poslužiteljskoj). Fatalan.
20	bad_record_mac	Pošiljatelj je primio zapis sa neispravnim autentikacijskim kôdom poruke (MAC). Fatalan.
30	decompression_failure	Informacija u zapisu se ne može ispravno dekomprimirati. Fatalan.
40	handshake_failure	Indicira da pošiljatelj nije u mogućnosti prihvatiti skup sigurnosnih parametara (npr. pošiljatelj nije zadovoljan sa primateljevim algoritmima za šifriranje i njihovom snagom). Fatalan.
41	no_certificate	Događa se kao odgovor na zahtjev za uvjerenjem ukoliko ne postoji odgovarajuće uvjerenje.
42	bad_certificate	Događa se ukoliko je zahtjev za uvjerenjem neuspješan (uvjerenje je neispravno ili je neispravan digitalni potpis).
43	unsupported_certificate	Događa se ukoliko pošiljatelj ne podržava određeni tip uvjerenja.
	certificiate_revoked	Događa se ukoliko pošiljatelj primi uvjerenje koje je već prije povučeno.
45	certicifate_expired	Događa se ukoliko pošiljatelj primi uvjerenje koje je isteklo.
46	certificate_unknown	Događa se ukoliko se prilikom obrade uvjerenja dogodi pogreška.
47	illegal_parameter	Događa se ukoliko pošiljatelj ustanovi da je neka vrijednost u protokolu za rukovanje nedozvoljene vrijednosti. Fatalan.

Tablica 2: *Popis izvanrednih događaja*

Razina	Ime	Opis
1	Warning (hrv. upozorenje)	SSL upozorenje znači da problem nije fatalan.
2	Fatal (hrv. fatalno)	SSL fatalni izvanredni događaji trenutno prekidaju trenutnu sjednicu.

Tablica 3: *Razine protokola za izvanredne događaje*

2.3. Protokol za promjenu načina šifriranja *(ChangeCipherSpec)*

Ovaj protokol se koristi za promjenu algoritma šifriranja. Za promjenu algoritma šifriranja klijent i poslužitelj moraju dogovoriti novi način šifriranja, isto kao i odgovarajuće ključeve.
Iako se način šifriranja obično mijenja na kraju protokola za rukovanje, on se može promijeniti u bilo kojem času.

2.4. Protokol za rukovanje (*Handshake*)

Prilikom spajanje klijenta sa SSL poslužiteljem inicira se protokol za rukovanje. Njime se definiraju protokoli koji će biti korišteni u daljnjoj komunikaciji, određuju se kriptografski algoritmi, obavlja se autentikacija strana, isto tako korištenjem kriptografije temeljene na javnom ključu kreira se *glavni tajni* ključ iz kojeg se izvode ostali ključevi za šifriranje i autentikaciju.
Glavni tajni ključ za svaku SSL sjednicu kreira poslužitelj koristeći pri tome inicijalni glavni ključ koji je poslao klijent. Uz pomoć glavnog tajnog ključa generiraju se četiri druga ključa:

- ključ za šifriranje podataka koji se šalju od klijenta prema poslužitelju,
- ključ za šifriranje podataka koji se šalju od poslužitelja prema klijentu,
- autentikacijski ključ za slanje podataka koji se šalju od klijenta prema poslužitelju,
- autentikacijski ključ za slanje podataka koji se šalju od poslužitelja prema klijentu.

Protokol za rukovanje sastoji se sljedećih koraka, odnosno razmjena poruka između klijenta i poslužitelja. Opcionalni koraci su u zagradama.

1. Klijent otvara komunikaciju i šalje *ClientHello*.
2. Poslužitelj šalje *ServerHello*.
3. {Poslužitelj šalje poslužiteljsko uvjerenje.}
4. {Poslužitelj šalje *ServerKeyExchange*.}
5. {Poslužitelj šalje *CertificateRequest*.}
6. {Klijent šalje klijentsko uvjerenje.}
7. Klijent šalje *ClientKeyExchange*.
8. {Klijent šalje *CertificateVerify*.}
9. Oba, klijent i poslužitelj šalju *ChangeCipherSpec* poruke.
10. Oba, klijent i poslužitelj šalju završne poruke.

S iznimkom tajnih ključeva koji su šifrirani s primateljevim javnim ključem, cijeli protokol se izvodi otvoreno. Tajni ključevi se zatim koriste za svaku daljnju komunikaciju.

2.4.1. ClientHello

ClientHello poruka sadrži informacije opisane u tablici 4.

Polje	Opis
ProtocolVersion client_version	Najnovija SSL verzija koju klijent podržava.
Random random	Slučajna struktura (sastoji se od 32-bitne vremenske značke i 28 okteta generiranih od strane sigurnog generatora slučajnih brojeva).
SessionID session_id	Sjednička identifikacija (ID). Polje je prazno prilikom zahtjeva za uspostavljanje nove sjednice, ukoliko nije tada to znači da klijent pokušava obnoviti prethodnu sjednicu.

Polje	Opis
	Klijent može specificirati vrijednost 0 i tako inzistirati na novoj sjednici iz sigurnosnih razloga.
CipherSuite ciper_suites<1..216-1>	Popis načina šifriranja koje klijent podržava.
CompressionMethod compression_methods<1..28-1>	Popis načina kompresije koje klijent podržava.

Tablica 4: *Sadržaj ClientHello poruke*

Nakon što je poslao *ClientHello*, klijent čeka *ServerHello* poruku.

2.4.2. ServerHello

Kada SSL poslužitelj primi *ClientHello* odgovara sa *handshake_failure* izvanrednim događajem ili sa *ServerHello* porukom. *ServerHello* poruka sadrži informacije opisane u tablici 5.

Polje	Opis
ProtocolVersion client_version	SSL verzija koju koristi klijent.
Random random	Slučajna struktura (sastoji se od 32-bitne vremenske značke i 28 okteta generiranih od strane sigurnog generatora slučajnih brojeva).
SessionID session_id	Sjednička identifikacija (ID). Ovo polje nije nikad prazno. Ukoliko se podudara sa session_id poljem iz ClientHello poruke, to znači da će prethodna SSL sjednica biti obnovljena. Inače session_id sadrži ID nove sjednice.
CipherSuite ciper_suites	Način šifriranja odabran od poslužitelja za tekuću sjednicu.
CompressionMethod compression_methods	Način kompresije odabran od poslužitelja za tekuću sjednicu.

Tablica 5: *Sadržaj ServerHello poruke*

Valja uočiti da poslužitelj odlučuje način šifriranja i kompresije koje će biti korištene u SSL sjednici. Ukoliko SSL poslužitelj nema implementirane ili ne želi koristiti niti jedan od načina šifriranja ili kompresije koje je ponudio klijent, poslužitelj jednostavno može poslati *handshake_failure* poruku i okončati sjednicu.

2.4.3. Poslužiteljsko uvjerenje

Nakon slanja *ServerHello* poruke poslužitelj može poslati svoje uvjerenje. Uvjerenje se sadrži jedno ili više X.509 v1, v2 ili v3 uvjerenja. (Ukoliko poslužitelj koristi Foretzza način šifriranja uvjerenje koje se šalje je modificirano X.509 uvjerenje).

2.4.4. ServerKeyExchange

Poslužitelj šalje ovu poruku samo ukoliko ne posjeduje uvjerenje ili se ono koristi za digitalne potpise. To se može dogoditi samo u tri slučaja:

- poslužitelj koristi Diffie-Hellman-ov protokol razmjene ključeva,
- poslužitelj koristi RSA, ali samo za digitalne potpise,
- poslužitelj koristi Foretzza/DMS način šifriranja.

2.4.5. CertificateRequest

Ukoliko poslužitelj želi autentikaciju klijentske strane, može poslati zahtjev za uvjerenjem (*CertificateRequest*) koji se sastoji od pet elemenata opisanih u tablici 6.

Polje	Opis
ClientCertificateType certificate_types<1..28-1>	Tipovi uvjerenja koje poslužitelj traži.
Random random	Slučajna struktura (sastoji se od 32-bitne vremenske značke i 28 okteta generiranih od strane sigurnog generatora slučajnih brojeva).
SessionID session_id	Sjednička identifikacija (ID). Ovo polje nije nikad prazno. Ukoliko se podudara sa session_id poljem iz ClientHello poruke, to znači da će prethodna SSL sjednica biti obnovljena. Inače session_id sadrži ID nove sjednice.
CipherSuite ciper_suite	Način šifriranja odabran od poslužitelja za tekuću sjednicu.
CompressionMethod compression_methods	Način kompresije odabran od poslužitelja za tekuću sjednicu.

Tablica 6: *Sadržaj CertificateRequest poruke*

2.4.6. Klijentsko uvjerenje

Ukoliko je poslužitelj to tražio, klijent šalje bilo koje uvjerenje od zatraženih. Ukoliko takovih uvjerenja nema, klijent šalje *no_certificate* poruku o izvanrednom događaju.
Na poslužitelju je da odluči što da učini ukoliko primi no certificate poruku; može nastaviti sjednicu sa anonimnim klijentom ili prekinuti vezu slanjem *handshake_failure* poruke.

2.4.7. ClientKeyExchange

Klijent može poslati jednu od tri vrste poruka za razmjenu ključeva, ovisno o tome koji je algoritam razmjene javnih ključeva izabran. Informacije koje su sadržane u poruci, ovisno o algoritmu opisane su u tablici 7.

Polje	Opis
Za Diffie-Hellmanovu razmjenu ključeva: opaque dh_Yc<1..216-1> Signature signature	 Klijentska javna Diffie-Hellmanova vrijednost (Yc) Digitalni potpis parametara.
Za RSA: ServerRSAarams params Structure signed_ params	 Poslužiteljski RSA parametri. Digitalni potpis parametara.
Za Foretzza/DMS: ServerForezzaParams params	 Poslužiteljski Foretzza parametri.

Tablica 7: Sadržaj ClientKeyExchange poruke

2.4.8. CertificateVerify

Ukoliko je klijent poslao svoje uvjerenje koje ima mogućnost digitalnog potpisivanja, nakon toga šalje *CertificateVerify* poruku. Ta poruka se sastoji od dva autentikacijska kôda, jedan kôd se računa sa MD5 algoritmom, a drugi sa SHA algoritmom.

```
Certificate.Verify.signature.md5_hash
      MD5(MAC_write_secret + pad2 +
            MD5(MAC_write_secret + pad1 + seq_num +
                  SSLCompressed.type + SSLCompressed.length +
                  SSLCompressed.fragment))

Certificate.Verify.signature.sha_hash
      SHA(MAC_write_secret + pad2 +
            SHA(MAC_write_secret + pad1 + seq_num +
```

```
SSLCompressed.type + SSLCompressed.length +
SSLCompressed.fragment))
```

2.4.9. ChangeCipherSpec

Nakon što je poslana poruka *CertificateVerify*, šalje se *ChangeCipherSpec* poruka. Nakon što je poslana, sve ostale poruke se šifriraju i komprimiraju prema odabranom načinu šifriranja odnosno komprimiranja.

2.4.10. Završna poruka

Na kraju klijent i poslužitelj šalju završne poruke. Završna poruka sastoji se od informacija opisanih u tablici 8.

Polje	Opis
opaque md5_hash[16]	16-oktetna MD5 vrijednost
opaque md5_hash[20]	20-oktetna SHA vrijedost

Tablica 8: *Sadržaj završne poruke*

Vrijednosti se računaju prema jednadžbama opisanim u tablici na temelju svih informacija poslanih prethodno. Završna poruka provjerava da li su klijent i poslužitelj pravilno sinkronizirani. Ukoliko nisu SSL veza se okončava.
Nakon što je poslana završna poruka protokola za rukovanje mogu se izmjenjivati podaci. Svi podaci se dijele u posebne poruke SSL sloja zapisa. Tako stvorene poruke se komprimiraju i šifriraju sukladno odabranim načinima kompresije i šifriranja.