20 gadi kopā ar *SSL/TLS*

Ivars Šūba

galvenais IS drošības administrators

Latvijas Banka

Esi drošs-2

Konferenču centrs “Citadele”

03.12.15

❖ ATSKATS VĒSTURĒ

SSL -Secure Socket Layer

TLS -Transport Layer Security

Definīcija: *"**Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communication security over a computer network"*

SSLv2 – Nov 1994, Netscape Navigator 1.1 Mar 1995 [1], *PRNG* uzbrukums(atslēgu entropija 2^{47}) [2]

SSLv3 – Q4 1995, Netscape Navigator 2

Netscape ->> IETF (Microsoft ietekmē)

Microsoft PCT(Private Communication Technology) balstās uz *SSLv2, IE* un *IIS*

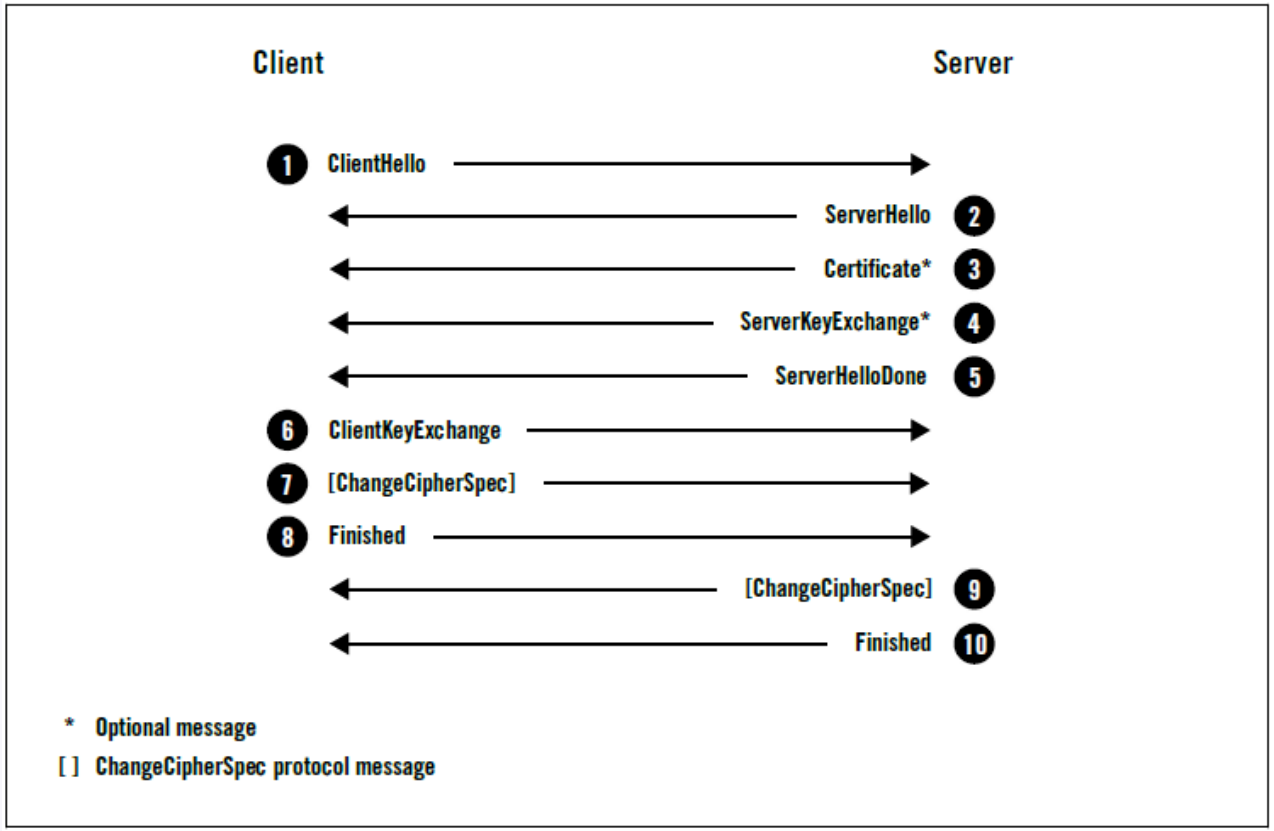
TLSv1.0 – Jan 1999, RFC 2246

TLSv1.1 – Apr 2006, TLS Extensions, savs *IV* katrā blokā, aizsardzība pret *"padding oracle "* uzbrukumiem, *RFC 4346*

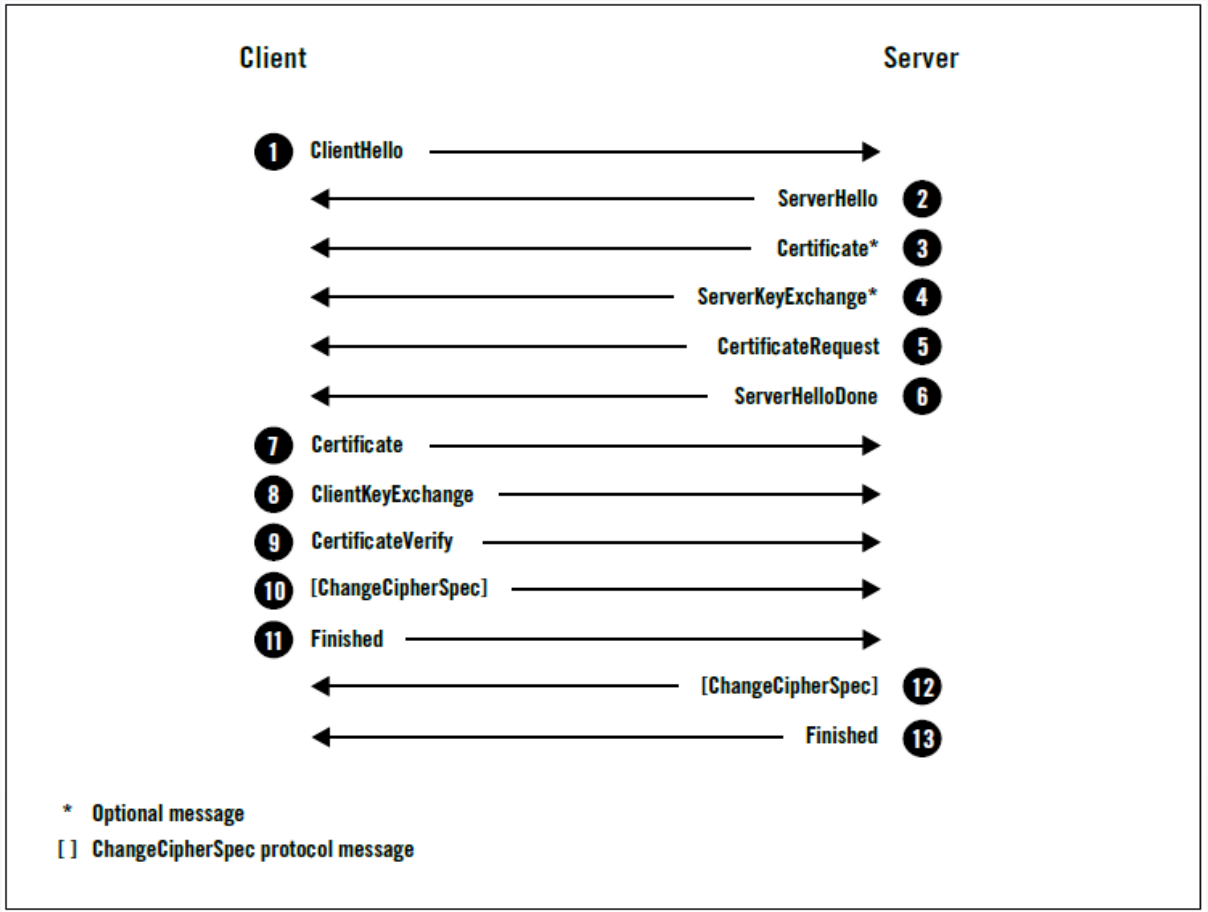
TLSv1.2 – Aug 2008, AEAD(Authenticated Encryption with Associated Data - autentificētā šifrēšana), *RFC 5246*

PROTOKOLA ARHITEKTŪRA(ĪSUMĀ) [3]

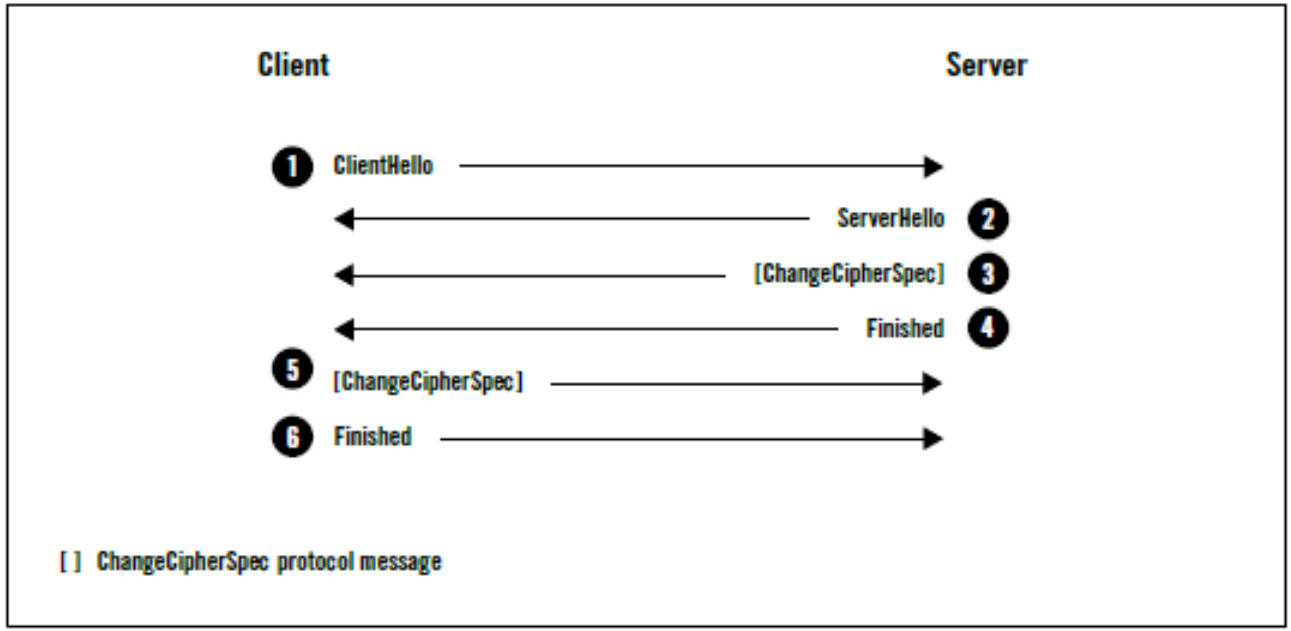
- PILNĀ SAROKOŠANĀS AR SERVERA AUTENTIFIKĀCIJU



PILNĀ SAROKOŠANĀS AR KLIENTA-SERVERA AUTENTIFIKĀCIJU



SAĪSINĀTĀ SAROKOŠANĀS – LIETO LAI ATSĀKTU JAU NODIBINĀTU SESIJU



PIELIETOJUMI

- Tīmekļa industrija *(https)*
- *SSL*-izētie protokoli *POP3S, IMAP4S, FTPS, LDAPS, StartTLS u.c.*
- RADIUS protokola autentifikācijas paplašinājumi *(eap-tls, eap-ttls, eap-peap-mschapv2)*
- *SSL VPN*-i (*OpenVPN*, izmanto *DTLS* protokolu, *Check Point*)
- *P2P(point-to-point)* protokoli *(Microsoft SSTP)*
- *IKEv2* , kā *IPSec* sastāvdaļa (*Win7 Agile VPN client*, mobilās ierīces , kopš *iOS 9.0* un *Windows Phone 8.1 eap-tls, eap-peap-mschapv2* atbalsts)

PROTOKOLU IEVAINOJAMĪBAS

- *Analysis of the SSL 3.0 Protocol, B.Schneier un D.Wagner 1996* [4]
- Nedroša sarunas atsākšana *(Insecure Renegotiation) – M.Ray 2009* [5], līdz Q4 2011 industrija *TLS* salaboja!
- *BEAST (Browser Exploit Against SSL and TLS), Sep 2011*[6] - ietekmē *SSL 3.0* un *TLS 1.*0 versijas. Klienta puses ievainojamība!
- *SSL/TLS* datu kompresija - blakus kanāla uzbrukumi

  - *CRIME(Compression Ratio Info-leak Made Easy), Sep 2012*[7] – darbojas ar *TLS/SPDY* kompresiju

  - *TIME(Timing Info-leak Made Easy), Mar 2013*[8] – darbojas mērot *RTT* starp klientu un serveri

  - *BREACH(Browser Reconnaissance & Exfiltration via Adpative Compression of Hypertext), Aug 2013*[9] – darbojas ar *HTTP response* kompresiju (*Request Rate Control* ar *WAF*, *response* garuma slēpšana, *CSRF token* maskēšana ar *XOR*)
- *Lucky13(5bytes of TLS header+ 8bytes of SN), Feb 2013*[10] - modificēts *“padding oracle”* uzbrukums pret *CBC* šifrēšanas algoritmiem, nepieciešams 2^{24} *TLS* sesijas, jāizmanto *AEAD*(piem., *AES-GCM*)
- *RC4, Mar 2013*[11] – lai uzlauztu 128-bitu atslēgu nepieciešams 2^{24} sesijas
- *Triple Handshake MiTM* uzbrukums, *Mar 2014*[12] - ietekmē pilno klienta-servera sertifikātu autentifikāciju, tuneletās autentifikācijas *(peap-tls, eap-ttls)* un *TLS* variantu ar *DHE* apmaiņu . Ietekmēja *Schannel, Chromium, NSS*, *SecureTransport* u.c. *ECDHE* atslēgu apmaiņa pasargā.

PROTOKOLU IEVAINOJAMĪBAS (TURPINĀJUMS)

- *POODLE(Padding Oracle On downgraded Legacy Encryption), Oct 2014*. Ietekmē *SSL 3.0* visus simetriskos *CBC* šifrēšanas algoritmus., dažas *TLS 1.0* realizācijas (*F5* slodzes balansētāji, un *A10*).
  - aizsardzība pret versijas *“downgrade”* uzbrukumu – *TLS_FALLBACK_SCSV (Signaling Cipher Suite Value)*
  - obligāts pasākums - atspējot *SSL 3.0* lietošanu uz servera

REALIZĀCIJAS IEVAINOJAMĪBAS

- *PRNG Netscape, 1994*[1] - *SSL 2.0* entropija tikai 47 biti
- *Debian, May 2008*[12] - *PRNG* entropija tikai 16 biti!!!
- *Heartbleed, Apr 2014*[13] - ietekmēja *OpenSSL* versijas *1.0.1-1.0.1f*. *Heartbeat (D)TLS* protokola paplašinājums, *PMTU* noteikšanai, paredzēts tikai pēc pilnās sarokošanās
- *CCS(ChangeCipherSpec)* injekcijas ievainojamība, *Jun 2014*[14] – lai izmantotu (1) abām pusēm jāatbalsts *openssl*, (2)ietekmē *OpenSSL 1.0.1* kopu
- *FREAK (Factoring RSA Export Keys), Jan 2015*[15] - ietekmē servera 512-bitu *RSA* exporta atslēgas *(Openssl/SecuteTransport),* parakstītu ar ilgtermiņa *RSA* atslēgu (37% no 14milj. *ssl* severu! pamatā *CDN*)
- Aktīvie uzbrukumi pret nedrošu *DH* atslēgu apmaiņu

  - *Logjam, May 2015*[16] - *DHE-512* uzlaušanai nepieciešams 30 sec. izmantojot pirmskaitļošanu (1ned.pirmskaitļošana ar predefinētiem p un g grupām ar *NFS* metodi). Ietekmē *Group1*, *Group2 DHE* atslēgas. Stingri ieteicams migrēt uz *Group14* vai izmantot *ECDHE*.

  - *KCI (Key Compromise Impersonation), Jun 2015*[17] - Izmanto fiksētās klienta-servera *(EC)DH* atslēgas un *(certc, skc)* injekciju klienta storē kombinācijā ar *MiTM*. Ieteicams atteikties no fiksētājām *(EC)DH* atslēgām.
- *SSL DoS*[18] uzbrukums serverim ar *RSA* atslēgām *(sslsqueeze). RSA-2048* atslēgu apmaiņa servera pusē prasa 7X lielāku skaitļošanas apjomu nekā klienta pusē. Ieteicams pāriet uz *(EC)DHE* atslēgu apmaiņu vai *ECDSA* sertifikātu izmantošanu

REKOMENDĀCIJAS

- Protokoli: Serveriem *TLS1.1* un *TLS 1.2* atbalsts (*TLS 1.0* pēc nepieciešamības, savietojamībai ,bet ar *1/n-1 splitting* tehnoloģiju aizsardzībai pret *BEAST* uzbrukumiem, *Mac OS X 10.9 Mavericks, 10.8.5 Mountain Lion*)
- *TLS* kompresija jāatspējo *un HTTP* kompresijas ietekme jāmazina
- *OCSP responder* vietā izmantot *OCSP stapling*
- *Session Cache* vietā izmantot *Session Tickets*
- Iespējot *HSTS (HTTP Strict Transport Security)* – aizsardzība pret *SSLstrip* uzbrukumiem
- Jāizmanto *PFS* ar 2048–bitu *DHE* vai *ECDHE* atslēgas
- Sākt izmantot *ECDSA* sertifikātus *(P-384)*(Bez *KU(Key Usage) KeyAgreement* karodziņa!)
- Atspējot *EXP* kriptogrāfiju *RC4* un *MD5* izmantošanu *HMAC* un *PRF* veidošanā

  SSLCipherSuite HIGH:MEDIUM:!EXP!MD5:!RC4
  SSLProxyCipherSuite HIGH:MEDIUM:!EXP!MD5:!RC4

REKOMENDĀCIJAS (TURPINĀJUMS)

- Šifrēšanas algoritmi:

Šifrēšanas algoritmu konfigurācija izmanto tikai *PFS* un nodrošina labāko veiktspēju

SSLCipherSuite
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES128-SHA
DHE-RSA-AES256-SHA
DHE-RSA-AES128-SHA256
DHE-RSA-AES256-SHA256
EDH-RSA-DES-CBC3-SHA

ATSAUCES

[1] - http://tim.dierks.org/2014/05/security-standards-and-name-changes-in.html

[2] - http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html

[3] – Ivan Ristic, “Bulletproof SSL and TLS”, Feisty Duck, 2015

[4] - https://www.schneier.com/paper-ssl.pdf

[5] - http://www.g-sec.lu/practicaltls.pdf

[6] - http://antoanthongtin.vn/Portals/0/TempUpload/pProceedings/2014/9/26/tetcon2012_juliano_beast.pdf

[7] - https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2012/september/details-on-the-crime-attack/

[8] - https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf

[9] - https://media.blackhat.com/us-13/US-13-Prado-SSL-Gone-in-30-seconds-A-BREACH-beyond-CRIME-Slides.pdf

[10] - http://www.isg.rhul.ac.uk/tls/Lucky13.html

[11] - http://www.isg.rhul.ac.uk/tls/

[12] - http://www.debian.org/security/2008/dsa-1571

[13] - https://en.wikipedia.org/wiki/Heartbleed

[14] - http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html

[15] - http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

[16] - https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

[17] - https://www.usenix.org/system/files/conference/woot15/woot15-paper-hlauschek.pdf

[18] - http://vincent.bernat.im/en/blog/2011-ssl-session-reuse-rfc5077.html

JAUTĀJUMI UN ATBILDES