یا ذاالامن والامان

امنیت داده و شبکه

امنیت وِب

مرتضی امینی - نیمسال دوم ۱۴۰۰-۱۳۹۹

فهرست مطالب

- تهدیدات وب و روشهای تامین امنیت
- معرفی SSL/TLS
- بسته پروتکل SSL
  - معماری و مفاهیم اولیه
  - پروتکلها
  - فازهای پروتکل Handshake
- بسته پروتکل TLS

خطرات تهدیدکننده وب

- با وجود سادگی راه‌اندازی خدمات مبتنی بر وب و گستردگی استفاده از مرورگرها، برنامه‌های تحت وب از پیچیدگی بالا و تهدیدات بالقوه فراوانی برخوردار است.
- نمونه‌ای از خطرات متداول:
  - حمله به وب سرورها
  - تهدید اعتبار برنامه‌های تجاری مهم
  - وجود کاربران عام و ناآشنا به خطرات امنیتی
  - دسترسی به حریم خصوصی افراد و آزار و اذیت آنها

دسته‌بندی حملات تهدیدکننده وب

- دسته‌بندی بر اساس تاثیر حمله
  - حملات منفعل: شنود، دسترسی به داده‌های حفاظت شده در وب سایت
  - حملات فعال: تغییر در داده‌های در حال انتقال، جعل کاربر یا سرور
- دسته‌بندی بر اساس مکان رخداد حمله
  - حملات سمت سرور
  - حملات سمت کاربر (مرورگر وب)
  - حملات به ترافیک شبکه وب: موضوع بحث این جلسه

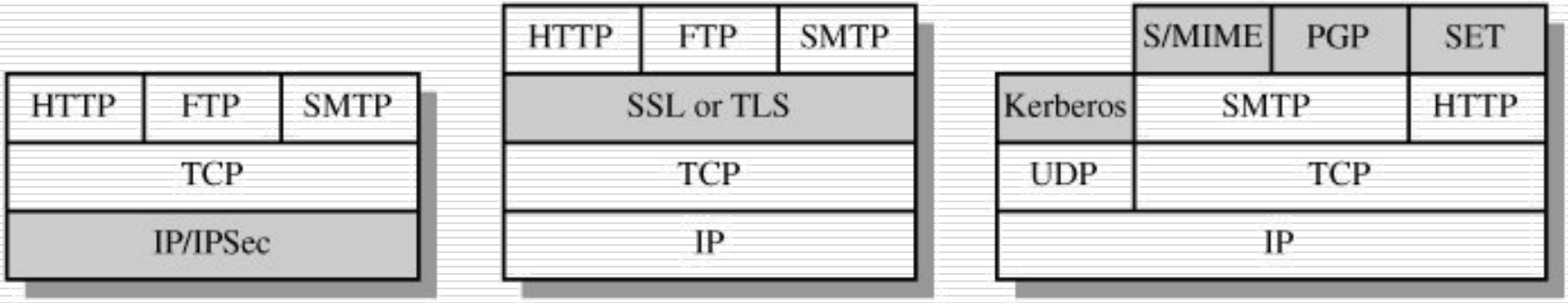
تهدیدات در وب

	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•Eavesdropping on the Net •Theft of info from server •Theft of data from client •Info about network configuration •Info about which client talks to server	•Loss of information •Loss of privacy	Encryption, web proxies
Denial of Service	•Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks	•Disruptive •Annoying •Prevent user from getting work done	Difficult to prevent
Authentication	•Impersonation of legitimate users •Data forgery	•Misrepresentation of user •Belief that false information is valid	Cryptographic techniques

روشهای مختلف تامین امنیت وب

- استفاده از IPSec
  - همه منظوره
  - پنهان از دید کاربران لایه بالاتر
  - سربار استفاده از IPSec (به خصوص در سمت کارفرما)
- استفاده از SSL/TLS
  - پنهان از دید برنامه‌های کاربردی
  - پشتیبانی مرورگرها و نیز بسیاری از وب سرورها
- سرویس‌های امنیتی وابسته به کاربرد خاص
  - تراکنش‌های مالی امن (SET)

روشهای مختلف تامین امنیت وب



(a) Network level (b) Transport level (c) Application level

فهرست مطالب

SSL/TLS – معرفی

- لایه امنیتی در بالای لایه انتقال
- ارائه شده توسط شرکت Netscape و نسخه ۳ آن نسخه استاندارد اینترنت است.
- سرویس قابل اطمینان انتها به انتها (end to end) و مبتنی بر TCP

SSL/TLS – معرفی

- نسخه‌ای بر مبنای UDP هم پیاده شده است که به آن Datagram Transport Layer Security (یا DTLS) می‌گویند.
- پروتکلهایی نظیر HTTP، FTP، SMTP و XMPP قادرند از SSL/TLS استفاده کنند.

پورتهای پیش‌فرض معروف

پروتکل	پورت عادی	پورت روی SSL/TLS
HTTP	۸۰	۴۴۳
XMPP	۸۰	۴۴۳
SMTP	۲۵ و ۵۸۷	۴۶۵
FTP	۲۰ و ۲۱	۹۸۹ و ۹۹۰
IMAP	۱۴۳	۹۹۳
POP3	۱۱۰	۹۹۵
LDAP	۳۸۹	۶۳۶
Telnet	۲۳	۹۹۲

تاریخچه

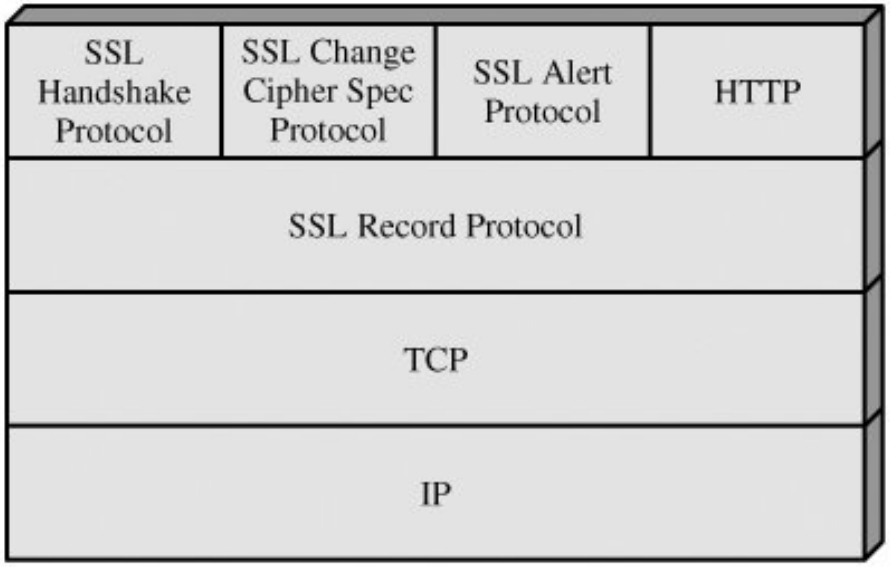
پروتکل	سال	توضیح
SSL 1.0	؟؟	داخلی Netscape – منتشر نشد – به شدت ناامن
SSL 2.0	۱۹۹۵	تعدادی ناامنی – از ۲۰۱۱ به بعد منسوخ محسوب می‌شود (RFC 6176)
SSL 3.0	۱۹۹۶	حمله POODLE به آن وارد است - از ۲۰۱۵ به بعد منسوخ محسوب می‌شود (RFC 7568)
TLS 1.0	۱۹۹۹	بر مبنای SSL 3.0 – قابلیت تنزل اتصال به SSL 3.0 و در نتیجه ناامنی
TLS 1.1	۲۰۰۶	رفع تعدادی از ناامنی‌های TLS 1.0
TLS 1.2	۲۰۰۸	افزودن برخی الگوریتمهای رمز به TLS 1.1
TLS 1.3	۲۰۱۸	حذف برخی الگوریتمهای رمز ضعیف – افزودن الگوریتمهای رمز جدید

فهرست مطالب

- تهدیدات وب و روشهای تامین امنیت
- معرفی SSL/TLS
- **بسته پروتکل SSL**
  - **معماری و مفاهیم اولیه**
  - پروتکلها
  - فازهای پروتکل Handshake
- بسته پروتکل TLS

SSL – معماری

- لایه اول بالای لایه انتقال و لایه دوم در لایه کاربرد
- لایه اول شامل زیرپروتکل Record و لایه دوم مربوط به سرویس‌های مدیریتی بوده و شامل زیرپروتکل‌های زیر است.



SSL – مفاهیم

- با استفاده از SSL یک نشست امن برقرار می‌شود و در طی یک نشست چند اتصال امن برقرار می‌شود.
- نشست (Session)
  - یک نشست SSL، یک پیوند بین کارفرما و کارگزار است.
  - هر نشست SSL با پروتکل Handshake شکل می‌گیرد.
  - هر نشست مجموعه‌ای از پارامترهای رمزنگاری است که بین چند اتصال می‌تواند به اشتراک گذارده شود، تا هزینه ارتباطات کاهش یابد.
- اتصال (Connection)
  - یک ارتباط همتا-به-همتای امن (رمزگذاری همراه با MAC) در لایه انتقال
  - هر اتصال به یک نشست نگاشت می‌شود.

فهرست مطالب

- خطرات تهدیدکننده وب
- روشهای مختلف تامین امنیت وب
- **بسته پروتکل SSL**
  - معرفی و مفاهیم اولیه
  - **زیرپروتکلها**
  - فازهای زیرپروتکل Handshake
- بسته پروتکل TLS

SSL – زیرپروتکل Record

زیرپروتکل SSL Record

دو سرویس برای SSL فراهم می‌کند:

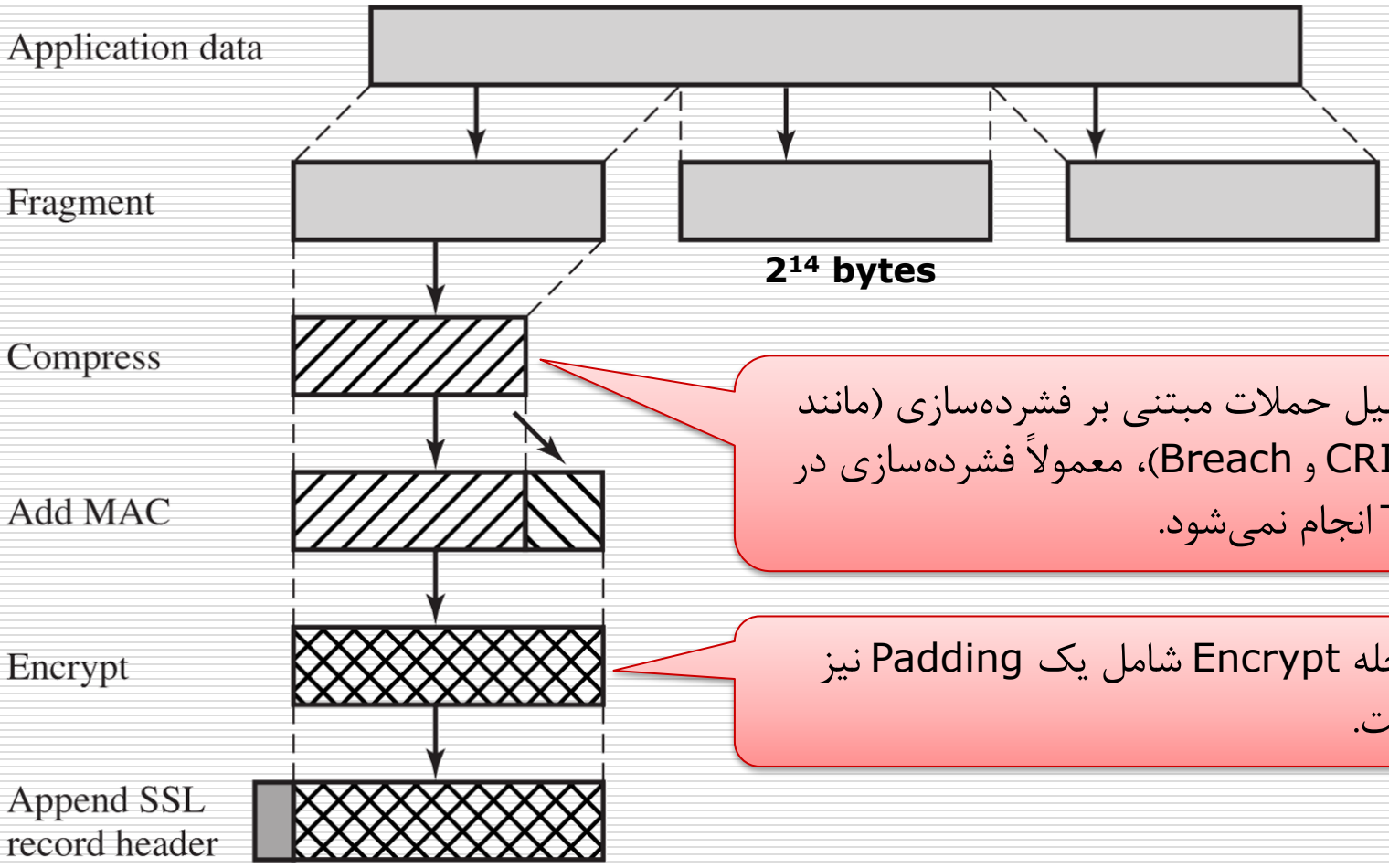
محرمانگی پیام

- با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به اشتراک گذاشته شده است.
- بسته به نسخه پروتکل استفاده از یکی از الگوریتم‌های IDEA، RC2-40، DES-40، DES، 3DES، Fortezza، RC4-40، RC4-128، AES، ...

صحت پیام

- تولید MAC با استفاده از کلید متقارن مخفی
- استفاده از SHA-1 یا MD5 یا خانواده SHA-2 یا در ترکیب با محرمانگی با مدهایی مانند GCM و CCM

اَعمال زیرپروتکل Record



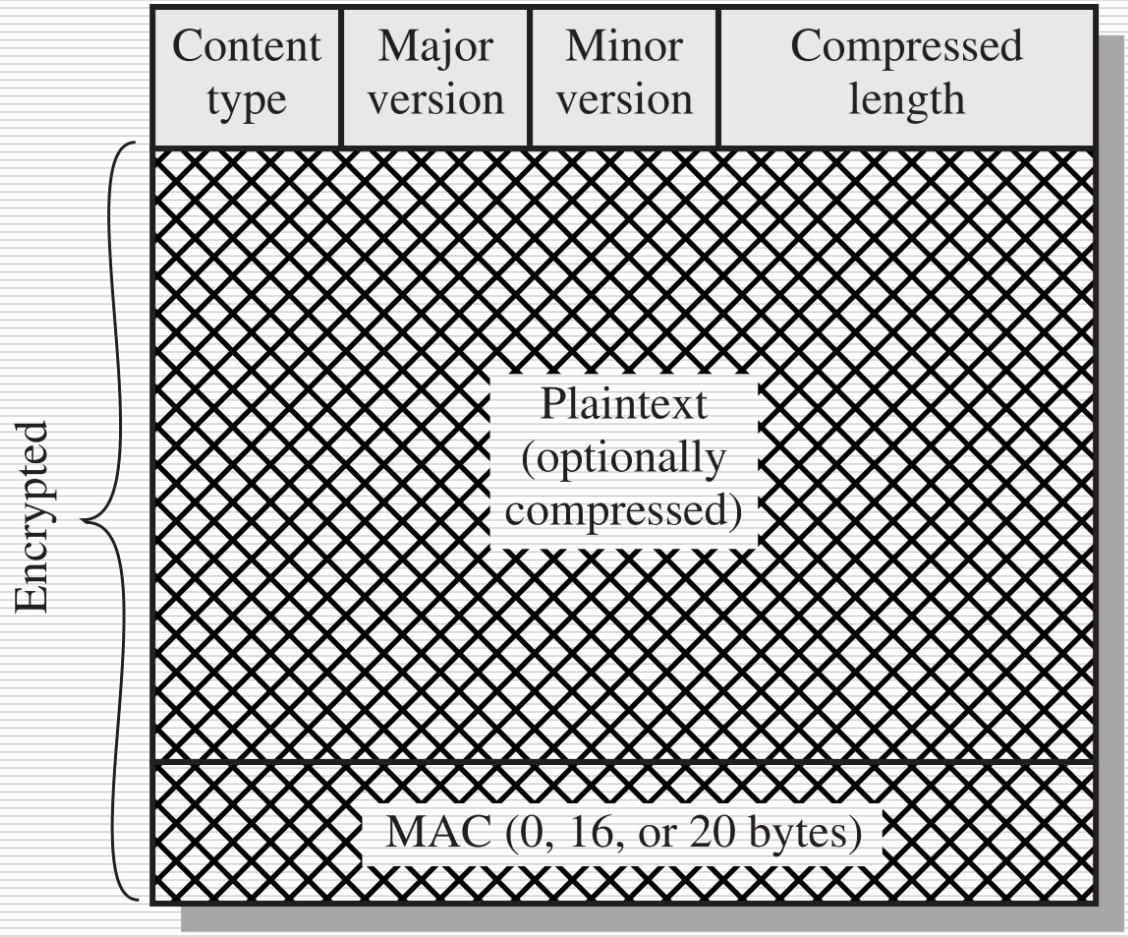
به دلیل حملات مبتنی بر فشرده‌سازی (مانند CRIME و Breach)، معمولاً فشرده‌سازی در TLS انجام نمی‌شود.

مرحله Encrypt شامل یک Padding نیز هست.

اَعمال زیرپروتکل Record

- قطعه‌بندی: تولید قطعاتی به طول 2^{14} یا کمتر .
- فشرده‌سازی: اختیاری و بدون از دست رفتن داده.
- تولید MAC: مشابه HMAC (ولی استفاده از concat به جای XOR) و روی ورودیهای زیر (در صورت استفاده از GCM و CCM متفاوت است):
  - (محتوای قطعه، طول قطعه، نوع فشرده‌سازی، شماره سریال)
- رمزنگاری: استفاده از رمز قطعه‌ای یا جریانی.
- اضافه‌کردن سرآیند: به ابتدای قطعه رمزشده می‌چسبد و شامل عناصر زیر است:
  - (نوع محتوا، نسخه SSL/TLS، طول داده فشرده شده)
  - نوع محتوا (Content Type) بیان کننده پروتکل استفاده کننده از این سرویس در لایه بالاتر است.

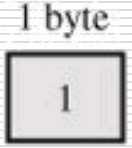
قالب SSL Record



SSL – زیرپروتکل Change Cipher Spec

زیرپروتکل Change Cipher Spec:

- یکی از ۳ زیرپروتکل لایه دوم SSL که از زیرپروتکل Record استفاده می‌کنند.
- شامل یک بایت است که حاوی مقدار ۱ است.
- در انتهای اجرای زیرپروتکل handshake، منجر به جایگزینی اطلاعات (حالت) یک نشست جدیدِ معلق (pending) به جای نشست فعلی می‌شود تا در اتصال جاریَ مورد استفاده قرار گیرد.

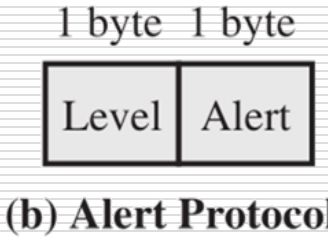


(a) Change Cipher Spec Protocol

SSL – زیرپروتکل Change Cipher Spec

زیرپروتکل SSL Alert:

- هشدارها و خطاهای مربوط به SSL را به طرف مقابل منتقل می‌کند.
- Level: شدت خطای پیش آمده؛ Warning یا Fatal.
- Alert: کد نمایانگر نوع خطا از جمله:
  - unexpected message, bad record mac, decompression failure, handshake failure



(b) Alert Protocol

- مانند بقیه داده‌های SSL فشرده‌سازی و رمزنگاری می‌شود.
- خطای Fatal موجب خاتمه یک اتصال و عدم ایجاد اتصال جدید در آن نشست می‌شود.

SSL – زیرپروتکل Change Cipher Spec

- نمونه‌هایی از خطاهای زیرپروتکل SSL Alert
  - unexpected_message
  - bad_record_mac
  - handshake_failure
  - certificate_revoked
  - certificate_expired
  - close_notify → برخی از پیام‌ها، پیام‌های کنترلی هستند.

SSL – زیرپروتکل Handshake

زیرپروتکل SSL Handshake

- پیش از انتقال هر نوع داده‌ای تحت SSL انجام می‌شود.
- با استفاده از آن کارفرما و کارگزار می‌توانند:
  - همدیگر را احراز اصالت کنند.
  - بر روی الگوریتم‌های رمزنگاری، تبادل کلید و توابع درهم ساز مورد استفاده **توافق** و کلیدهای رمزنگاری متقارن و نامتقارن را **تبادل** کنند.

(c) Handshake Protocol

انواع پیامهای پروتکل Handshake

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

فهرست مطالب

- خطرات تهدیدکننده وب
- روشهای مختلف تامین امنیت وب
- **بسته پروتکل SSL**
  - معرفی و مفاهیم اولیه
  - زیرپروتکلها
  - **فازهای زیرپروتکل Handshake**
- بسته پروتکل TLS

زیرپروتکل SSL Handshake

زیرپروتکل SSL Handshake

- شامل ۴ فاز اصلی زیر است:
  - مشخص کردن قابلیت‌های رمزنگاری (Cipher Suite) دو طرف
  - احراز اصالت کارگزار به کارفرما و مبادله کلیدهای آن
  - احراز اصالت کارفرما به کارگزار و مبادله کلیدهای آن
  - جایگزینی پارامترهای رمزنگاری جدید به جای قبلی و خاتمه توافق

زیرپروتکل Handshake – ۱
فاز تبیین توانمندیهای امنیتی

- ارسال پیغام Hello توسط کارفرما (آغازگر جلسه)
- پیشنهاد نسخه پروتکل: آخرین نسخه پشتیبانی شده توسط کارفرما
- پیشنهاد الگوریتم‌های رمزنگاری و درهم‌سازی مناسب و روش تبادل کلید آنها (Cipher Suite)
- پیشنهاد مکانیزم فشرده‌سازی مناسب
- انتخاب برترین الگوریتم رمزنگاری و فشرده‌سازی مورد توافق طرفین توسط کارگزار

۱–Handshake زیرپروتکل
فاز تبیین توانمندیهای امنیتی

```
▾ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 119
    Version: TLS 1.2 (0x0303)
  ▾ Random
      GMT Unix Time: Oct 11, 2105 18:06:07.000000000 Iran Standard Time
      Random Bytes: 66d6ef331b0b9071cdec232cc5ab501c9cabce9406e6ffb4...
    Session ID Length: 0
    Cipher Suites Length: 6
  ▾ Cipher Suites (3 suites)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Compression Methods Length: 1
  › Compression Methods (1 method)
    Extensions Length: 72
  › Extension: renegotiation_info
  › Extension: SessionTicket TLS
  › Extension: next_protocol_negotiation
  › Extension: Application Layer Protocol Negotiation
  › Extension: status_request
  › Extension: signature_algorithms
```

زیرپروتکل Handshake-۱
فاز تبیین توانمندیهای امنیتی

```
▾ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 49
    Version: TLS 1.2 (0x0303)
  ▾ Random
      GMT Unix Time: Oct  2, 2043 23:47:27.000000000 Iran Standard Time
      Random Bytes: 3338f1835d4e202a847a51f89e6017c8de2102b0091362c4...
    Session ID Length: 0
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Compression Method: null (0)
    Extensions Length: 9
  ▸ Extension: renegotiation_info
  ▸ Extension: SessionTicket TLS
```

زیرپروتکل Handshake – ۲ و ۳
فاز احراز اصالت و تبادل کلید

ارسال گواهی کارگزار برای کارفرما

- همراه با کلید عمومی (RSA) یا پارامترهای DH

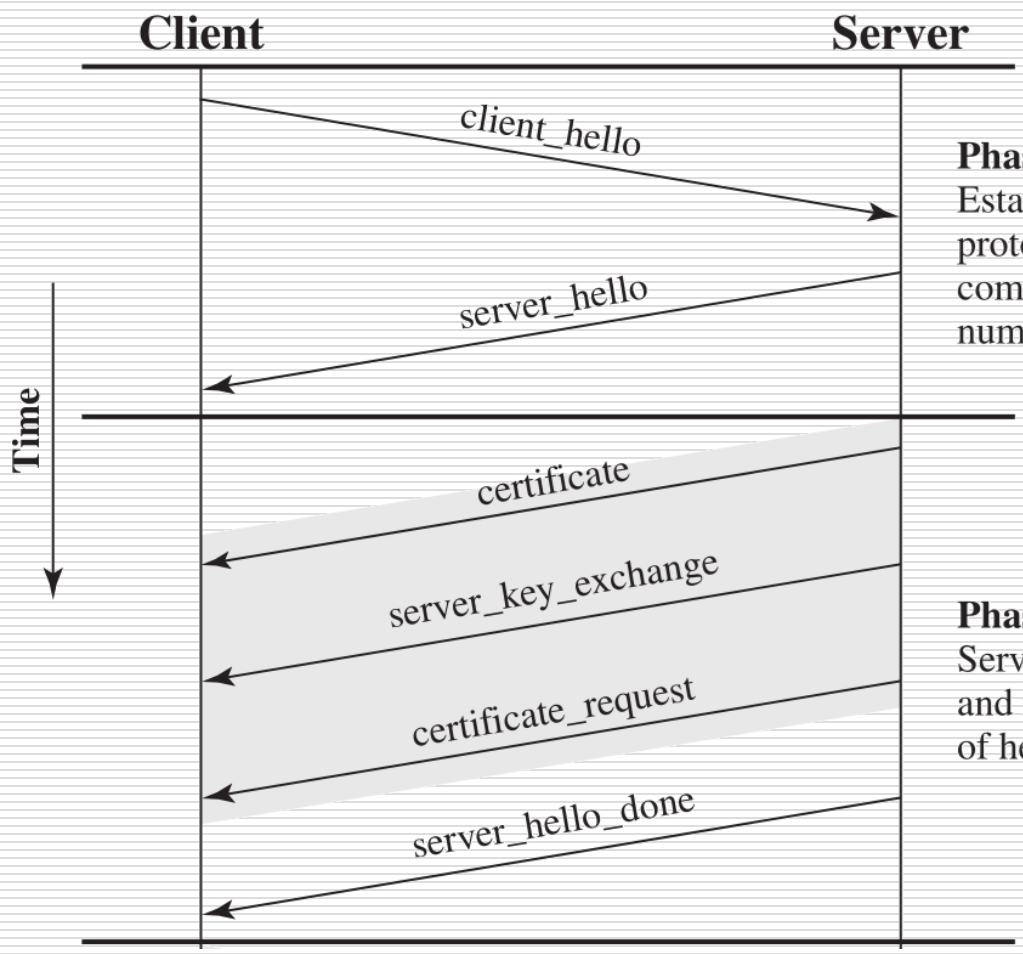
تولید و ارسال کلید سری

- کارفرما گواهی کلید عمومی کارگزار را وارسی می‌کند.
- کارفرما کلید سری را تولید کرده و رمزشده به کارگزار می‌فرستد.
- یا این که پارامترهای DH را ارسال می‌کند تا هر دو طرف کلید سری را محاسبه کنند.
- در صورت درخواست کارگزار، کارفرما گواهی کلید عمومی خود را به همراه امضای تمام پیام‌های ارسالی و دریافتی (برای احراز اصالت خود) به کارگزار می‌فرستد.

زیرپروتکل Handshake – ۴
فاز خاتمه

- فعال کردن زیرپروتکل تغییر مشخصات رمز (Change Cipher Spec)
  - کارفرما پیام پروتکل تغییر مشخصات رمز را برای کارگزار می‌فرستد.
  - کارگزار حالت خود را بروز کرده (با پارامترهای توافق شده در پروتکل Handshake) و پیام پروتکل تغییر مشخصات رمز را برای کارفرما ارسال می‌کند.
- پایان
  - ارسال پیام پایانی finished از کارفرما (همراه با پیام تغییر رمز بالا)
  - ارسال پیام پایانی finished از کارگزار (همراه با پیام تغییر رمز بالا)
  - آغاز تبادل اطلاعات به صورت محرمانه و با پارامترهای جدید

پروتکل SSL Handshake

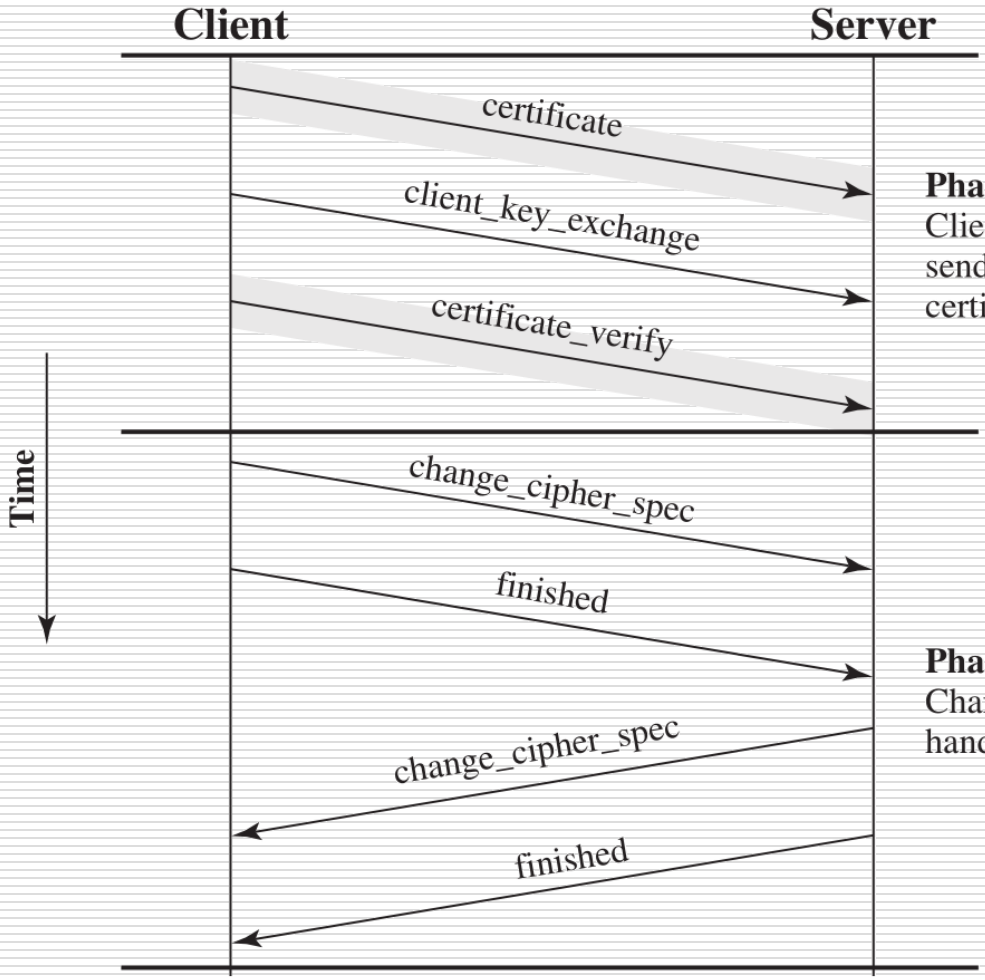


پیامهای خاکستری اختیاری یا وابسته به موقعیت هستند.

Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

پروتکل SSL Handshake



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

تبادل کلید

- نوع پروتکل مورد استفاده جهت تبادل کلید:
  - **توزیع کلید** (**Transport**): معمولاً مبتنی بر RSA
  - **توافق کلید:** معمولاً مبتنی بر DH
- DH با امنیتِ مساویِ RSA، شدیداً کندتر است.
- استفاده از DH با پارامترهای (کلیدهای) متفاوت برای هر نشست (Ephemeral DH)، به دلیل فراهم آوردن محرمانگی پیشرو ترجیح دارد.
- Ephemeral DH روی خمهای بیضوی (Elliptic Curves) معروف به ECDHE (E کوته‌نوشت Exchange) نیز دارای محرمانگی پیشرو است.

انواع مدل‌های اعتماد در SSL/TLS

- طرفین هیچ کلید مشترکی از هم ندارند (Anonymous DH)
- طرفین از هم کلید متقارن (Pre-Shared Key یا PSK) دارند و برای احراز اصالت (طرفین و پارامترهای عمومی) از این کلید استفاده می‌کنند.
- کارگزار، کارخواه، یا هر دو از هم گواهی دیجیتال دارند و از امضا برای احراز اصالت (طرفین و پارامترهای عمومی) استفاده می‌کنند.
  - مبتنی بر RSA (دو نوع: RSA فقط برای امضا؛ RSA برای امضا و رمز)
  - مبتنی بر DSA (دو نوع: DH پارامترهای ثابت؛ DH با پارامترهای متغیر)

Fixed DH

Ephemeral DH

انواع کلید

- کلیدی که در زیرپروتکل Handshake تبادل می‌شود، مقداری به نام Pre-Master Secret است.
- با استفاده از Pre-Master Secret، ابتدا Master Secret محاسبه می‌شود و از Master Secret شش مقدار مخفی محاسبه می‌شود:
- Client write MAC secret
- Server write MAC secret
- Client write encryption key
- Server write encryption key
- Client write encryption IV
- Server write encryption IV

SSL – جمع‌بندی

- SSL نیازهای امنیتی زیر را فراهم می‌کند:
  - محرمانگی داده
    - با استفاده از رمزنگاری متقارن
  - صحت داده
    - با استفاده از کد احراز اصالت داده
  - احراز اصالت کارگزار (و در صورت نیاز کارفرما)
    - بر اساس استاندارد X.509 یا رمز متقارن
- امروزه مهمترین کاربرد SSL در قرارداد HTTPS است.

فهرست مطالب

- خطرات تهدیدکننده وب
- روشهای مختلف تامین امنیت وب
- بسته پروتکل SSL
  - معرفی و مفاهیم اولیه
  - پروتکلها
  - فازهای پروتکل Handshake
- **بسته پروتکل TLS**

TLS (Transport Layer Security)

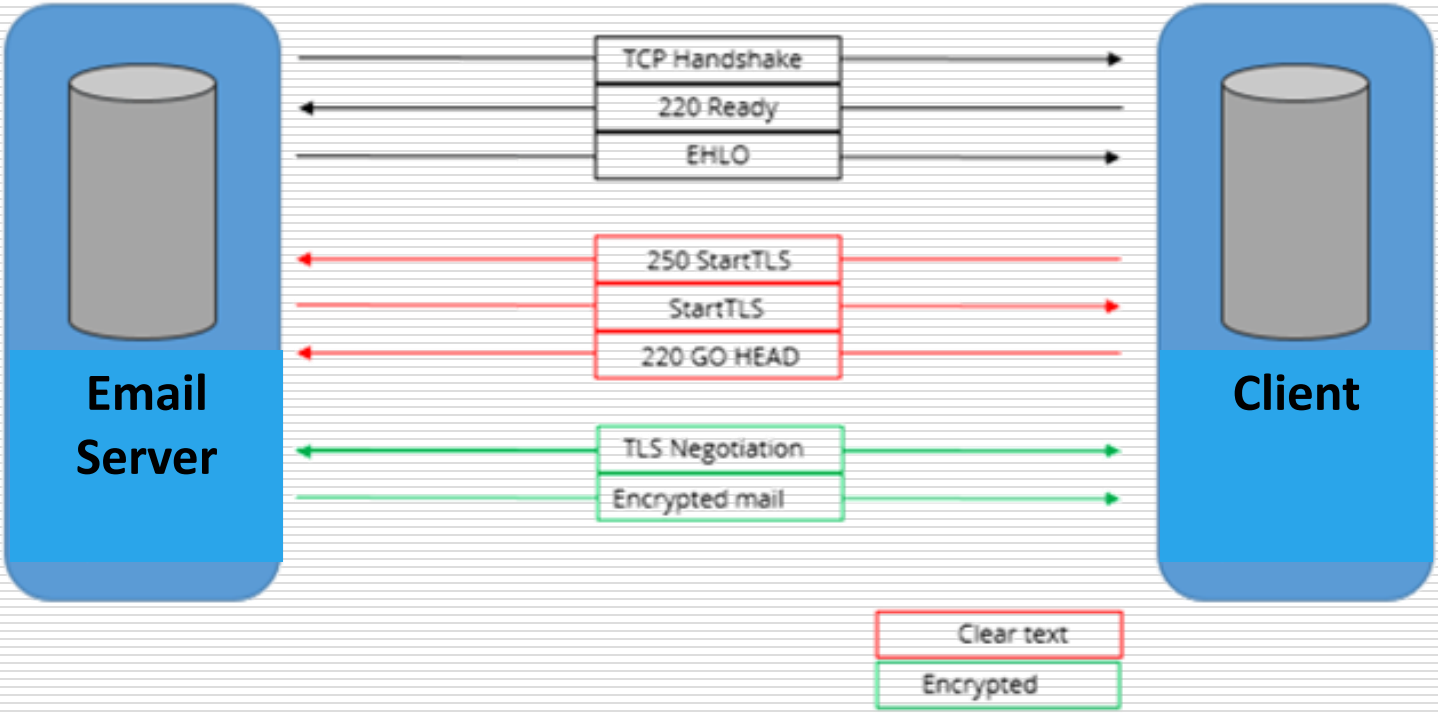
- یک استاندارد از IETF
- به دنبال ایجاد یک نسخه استاندارد اینترنتی از SSL است.
- نسخه اول آن (TLS 1.0) بسیار شبیه SSL نسخه ۳ بدون در نظرگرفتن تفاوت‌های جزئی زیر:
  - بهره گیری از HMAC واقعی در محاسبه MAC (استفاده از عملگر XOR).
  - در TLS کد خطای no-certificate قابل قبول نیست و مجموعه کد خطاها افزایش یافته است.
  - الگوریتم Fortezza از الگوریتم‌های توزیع کلید و رمزگذاری حذف شد.
  - . . .

فرمان STARTTLS

- فرمان STARTTLS افزونه‌ای بر پروتکلهای متن آشکار است، که با اجرای آن می‌توانند یک اتصال ناامن را به اتصالی امن با استفاده از SSL/TLS ارتقا دهند. **مثال:** SMTP:

```
S: <waits for connection on TCP port 25>
C: <opens connection>
S: 220 mail.example.org ESMTP service ready
C: EHLO client.example.org
S: 250-mail.example.org offers welcome
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <check result of negotiation>
C: EHLO client.example.org
```

فرمان STARTTLS



پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

amini@sharif.edu