



# یادداشتن و الامان

امنیت داده و شبکه

امنیت وب مبتنی بر **SSL/TLS**

مرتضی امینی - سیدمهدی خرازی

نیمسال اول ۱۴۰۴-۱۴۰۳



# فهرست مطالب

- تهدیدات وب
- معرفی SSL/TLS
- بسته پروتکل SSL
- معماری و مفاهیم اولیه
- پروتکلهای
- فازهای پروتکل Handshake
- بسته پروتکل TLS



# فهرست مطالب

□ تهدیدات و ب

□ معرفی SSL/TLS

□ بسته پروتکل SSL

■ معماری و مفاهیم اولیه

■ پروتکلهای

■ فازهای پروتکل Handshake

□ بسته پروتکل TLS



# دسته‌بندی حملات تهدیدکننده وب

- دسته‌بندی بر اساس مکان رخداد حمله
- حملات سمت سرور
- حملات سمت کاربر (مرورگر وب)
- حملات به ترافیک شبکه وب: **موضوع بحث این جلسه**



# فهرست مطالب

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



# SSL/TLS – معرفی

- لایه امنیتی در **بالای لایه انتقال**
- ارائه شده توسط شرکت Netscape و نسخه ۳ آن استاندارد اینترنت است.
- سرویس قابل اطمینان انتها به انتهای و مبتنی بر TCP
- نسخه‌ای بر مبنای UDP هم پیاده شده است که به آن Datagram می‌گویند.
- پروتکل‌هایی نظیر HTTP، FTP، XMPP و SMTP قادرند از SSL/TLS استفاده کنند.



# پورت‌های پیش‌فرض معروف

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



# تاریخچه

پروتکل	سال	توضیح
SSL 1.0	۹۹	داخلی <b>Netscape</b> – منتشر نشد – به شدت نامن
SSL 2.0	۱۹۹۵	تعدادی نامنی – از ۲۰۱۱ به بعد منسوخ محسوب می‌شود (RFC 6176)
SSL 3.0	۱۹۹۶	حمله <b>POODLE</b> به آن وارد است – از ۲۰۱۵ به بعد منسوخ محسوب می‌شود (RFC 7568)
TLS 1.0	۱۹۹۹	بر مبنای SSL 3.0 – قابلیت تنزيل اتصال به SSL 3.0 و در نتیجه نامنی
TLS 1.1	۲۰۰۶	رفع تعدادی از نامنی‌های 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



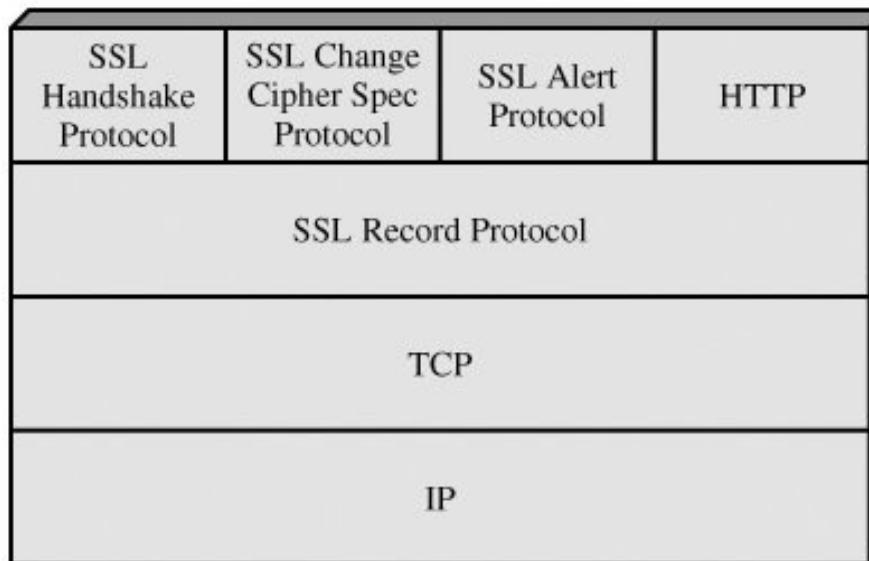
# فهرست مطالب

- تهدیدات وب و روش‌های تامین امنیت
- معرفی SSL/TLS
- بسته پروتکل SSL
- معماری و مفاهیم اولیه
  - پروتکلهای
  - 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 گذارد شود، تا هزینه ارتباطات کاهش یابد.

## □ اتصال (Connection)

- یک ارتباط همتا-به-همتای امن (رمزنگاری 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
  - زیرپروتکلهای Handshake
  - فازهای زیرپروتکل TLS



# Record - زیرپروتکل SSL

## □ زیرپروتکل SSL Record

دو سرویس برای SSL فراهم می‌کند:

### ■ محموله پیام

- با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به اشتراک گذاشته شده است.

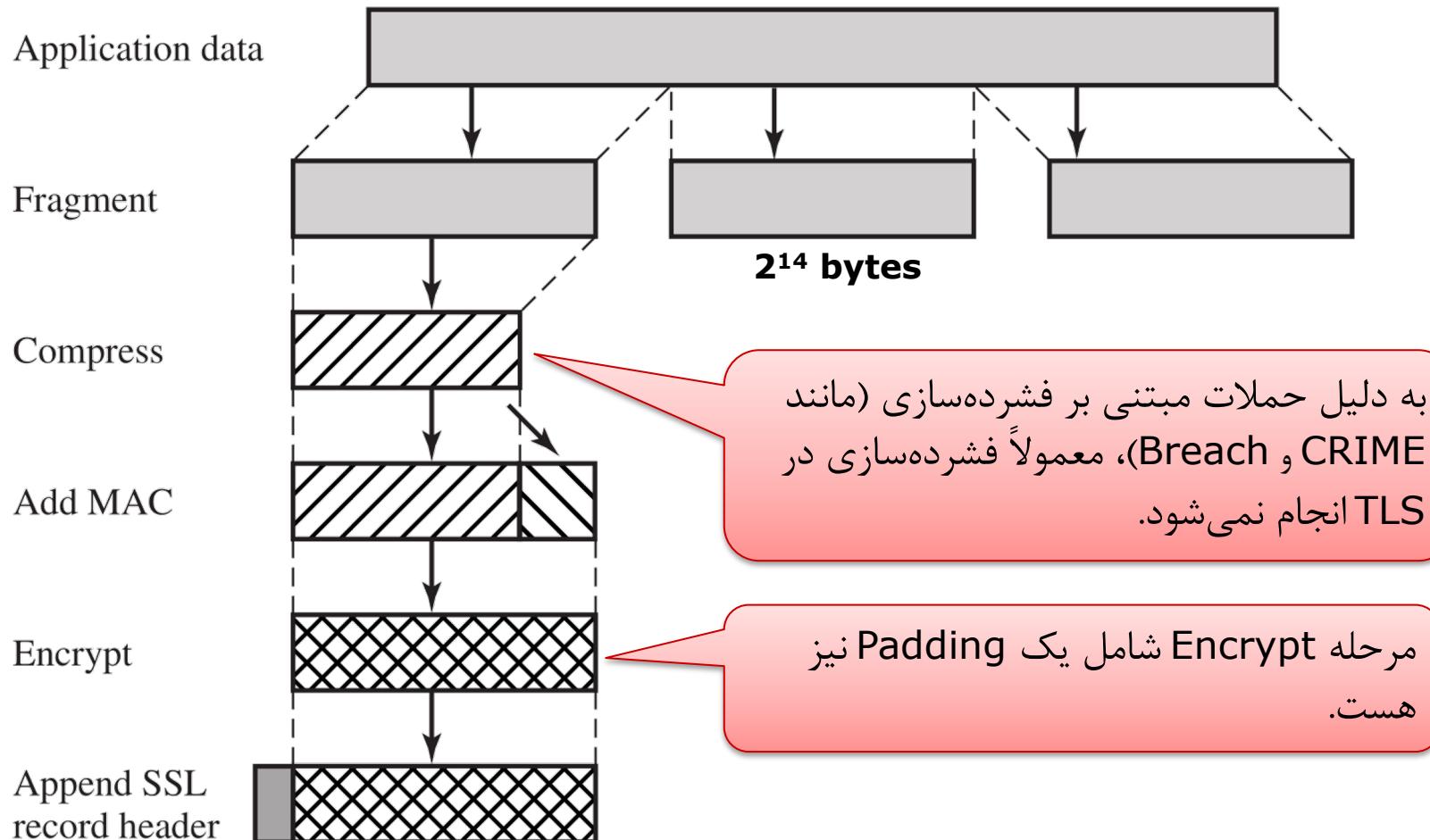
- بسته به نسخه پروتکل استفاده از یکی از الگوریتم‌های IDEA، DES-40، RC2-40، ...، AES، RC4-128، RC4-40، Fortezza، 3DES

### ■ صحت پیام

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



# أعمال زیرپروتوكل Record



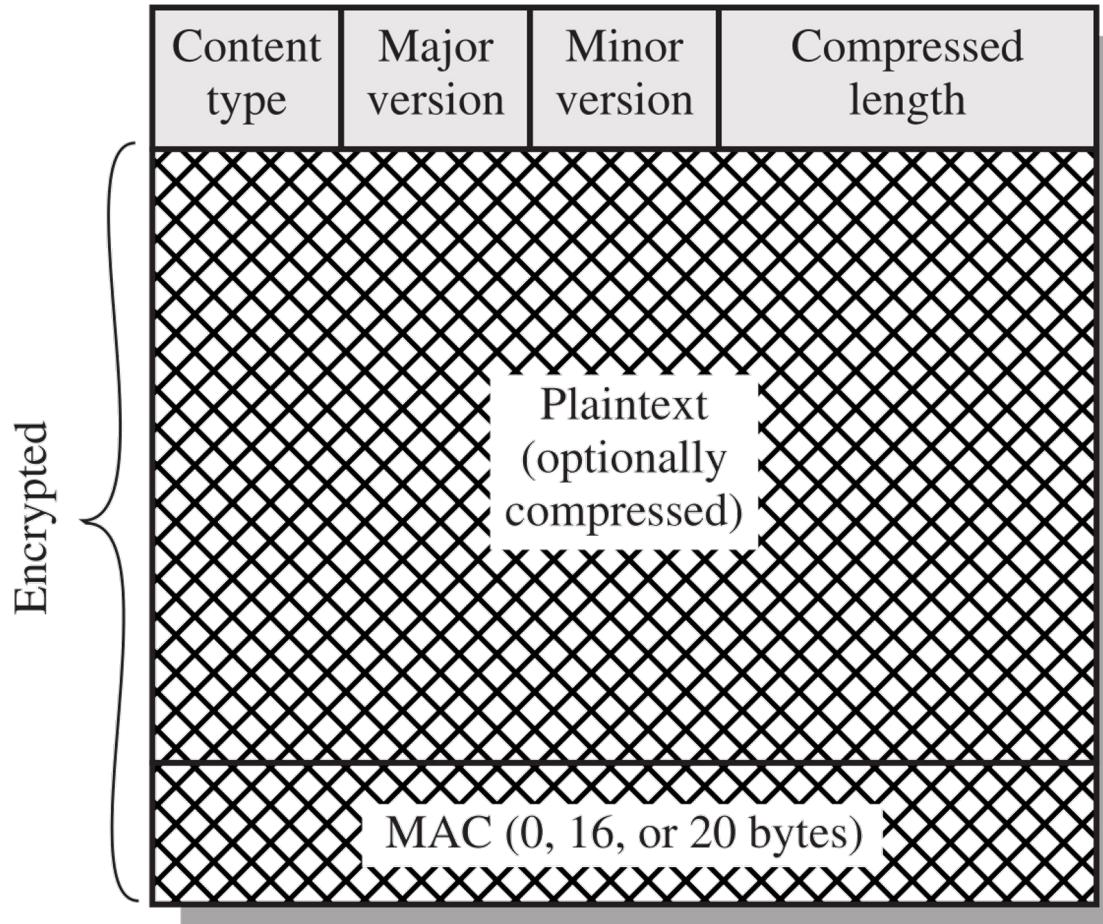


# أعمال زیرپروتکل Record

- قطعه‌بندی: تولید قطعاتی به طول ۲۱۴ یا کمتر.
- فشرده‌سازی: اختیاری و بدون از دست رفتن داده.
- تولید MAC: مشابه HMAC (ولی کمی متفاوت) 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.
- اضافه کردن 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

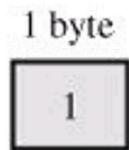




# Change Cipher Spec - زیرپروتکل SSL

## زیرپروتکل :Change Cipher Spec

- در انتهای اجرای زیرپروتکل handshake، منجر به جایگزینی اطلاعات (حالت) یک نشست جدید معلق (pending) به جای نشست فعلی می‌شود تا در اتصال جاری مورد استفاده قرار گیرد.



(a) Change Cipher Spec Protocol

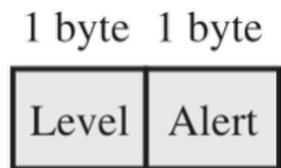


# Change Cipher Spec - زیرپروتکل SSL

## زیرپروتکل SSL Alert □

هشدارها و خطاهای مربوط به SSL را به طرف مقابل منتقل می‌کند. ■

.Fatal شدت خطای پیش آمده؛ Warning یا Level ■



کد نمایانگر نوع خطا از جمله: Alert ■

(b) Alert Protocol  
decompression unexpected message, bad record mac, □  
failure, handshake failure, certificate\_expired,  
certificate\_revoked

مانند بقیه داده‌های SSL پس از برقراری نشست، فشرده و رمز می‌شود. ■

خطای Fatal موجب خاتمه یک اتصال و عدم ایجاد اتصال جدید در آن نشست می‌شود. ■



# Handshake - زیرپروتکل SSL

## SSL Handshake □ زیرپروتکل

- 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 چکیده‌ساز مورد استفاده **توافق** و کلیدهای رمزنگاری متقارن و نامتقارن را **تبادل** کنند.

	1 byte	3 bytes	$\geq 0$ bytes
Type	Length	Content	

(c) Handshake Protocol



# فهرست مطالب

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



# زیرپروتکل SSL Handshake

## SSL Handshake □ زیرپروتکل

- 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



# ۱- Handshake فاز تبیین توانمندیهای امنیتی

- ارسال پیغام Client Hello توسط کارفرما (آغازگر جلسه)
  - پیشنهاد نسخه پروتکل: آخرین نسخه پشتیبانی شده توسط کارفرما
  - پیشنهاد الگوریتم‌های رمزنگاری و چکیده‌سازی مناسب و روش تبادل کلید آنها (Cipher Suite)
  - ارسال شناسه نشست و نانس (ترکیب مهر زمانی و یک مقدار تصادفی)
  - 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



# ۱ - Handshake زیرپروتکل 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) (highlighted)
  - Compression Method: null (0)
  - Extensions Length: 9
    - > Extension: renegotiation\_info
    - > Extension: SessionTicket TLS



# ذیروپروتکل 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 **کلید عمومی گواهی** خود را به همراه **امضای تمام پیام‌های ارسالی** و دریافتی (برای احراز اصالت خود) به کارگزار می‌فرستد.



# ۴ - Handshake فاز خاتمه

## □ فعال کردن زیرپروتکل تغییر مشخصات رمز (Change Cipher Spec)

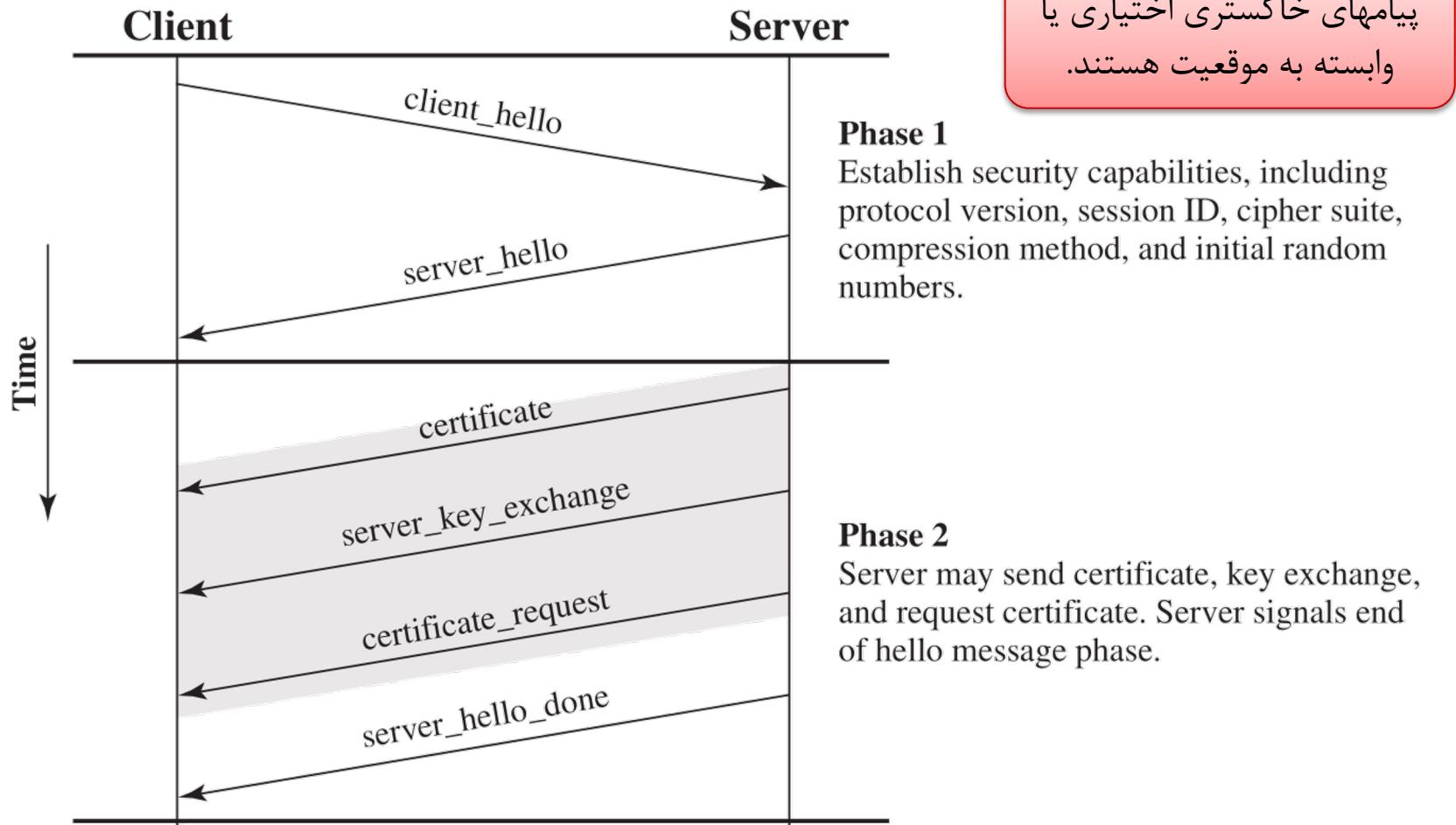
- کارفرما پیام پروتکل تغییر مشخصات رمز را برای کارگزار می‌فرستد.
- کارگزار حالت خود را بروز کرده (با پارامترهای توافق شده در پروتکل Handshake) و پیام پروتکل تغییر مشخصات رمز را برای کارفرما ارسال می‌کند.

## □ 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 محترمانه و با پارامترهای جدید

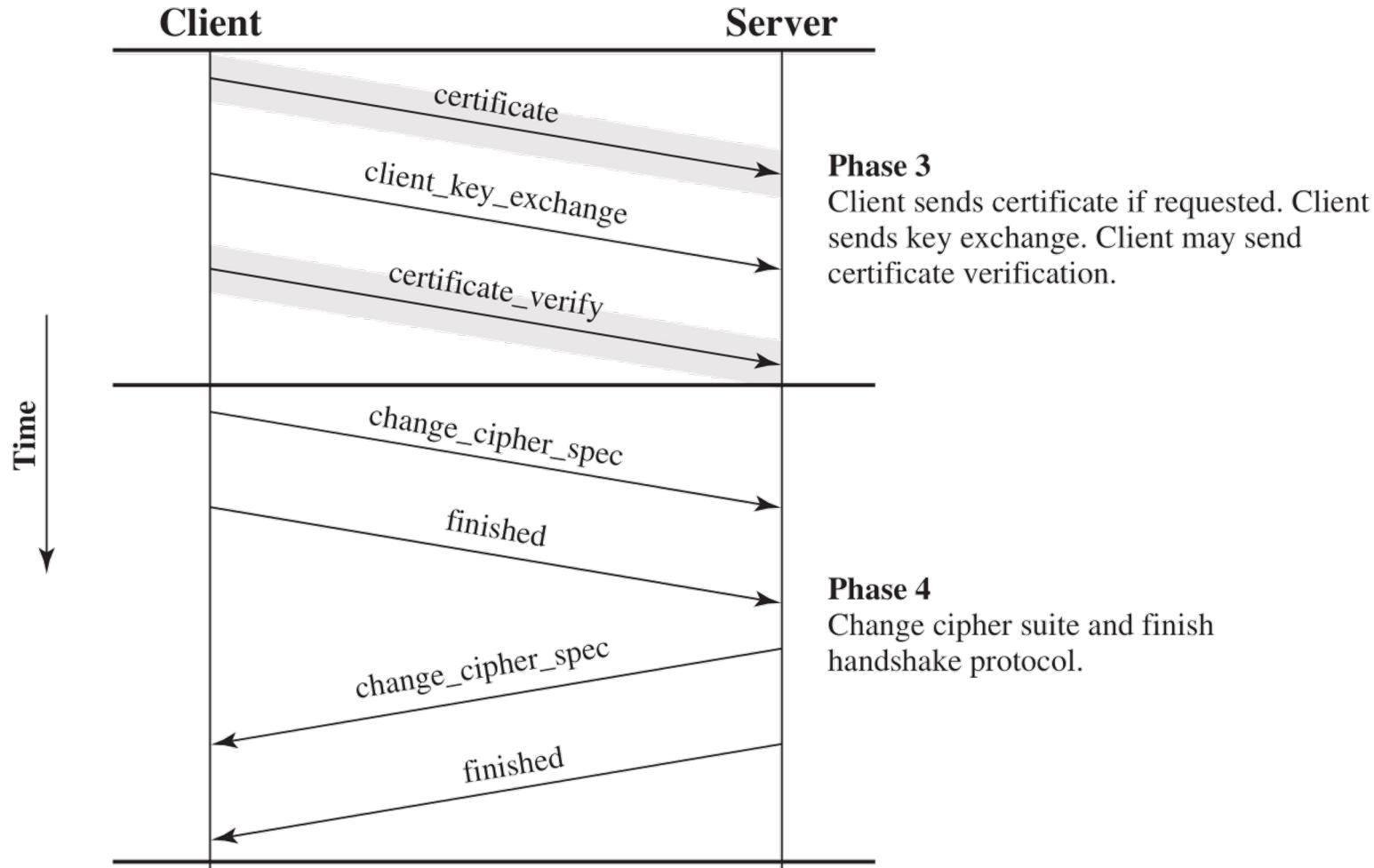


# پروتکل SSL Handshake





# پروتکل SSL Handshake





# تبادل کلید

□ انواع روش‌های تبادل کلید مورد استفاده:

■ توزیع کلید: معمولاً مبتنی بر RSA

■ توافق کلید: معمولاً مبتنی بر DH (و استفاده از امضا RSA یا DSS برای احراز اصالت) با انواع زیر:

□ DH با پارامترهای ثابت (Fixed DH): پارامترهای عمومی در گواهی امضاء شده توسط CA به طور ثابت درج شده است.

□ DH با پارامترهای متغیر (Ephemeral DH): استفاده از DH با پارامترهای عمومی (کلیدهای) متفاوت برای هر نشست (به دلیل فراهم آوردن محرومگی پیشرو ترجیح دارد)

□ ECDHE روی خمها بیضوی (Elliptic Curves): معروف به Ephemeral DH (کوتنهنوشت Exchange) نیز دارای محرومگی پیشرو است.



# 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
    - مقابله با حمله تکرار در سطح داده‌های ارسالی
- 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
- پروتکلهای
- 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 نظر گرفتن تفاوت‌های جزئی زیر:
  - بهره گیری از HMAC واقعی در محاسبه MAC
  - در TLS کد خطای no-certificate قابل قبول نیست و مجموعه کد خطاهای افزایش یافته است.
  - الگوریتم Fortezza از الگوریتم‌های توزیع کلید و رمزگذاری حذف شد.
- در حال حاضر تنها استفاده از TLS 1.2 و TLS 1.3 توصیه می‌شود.



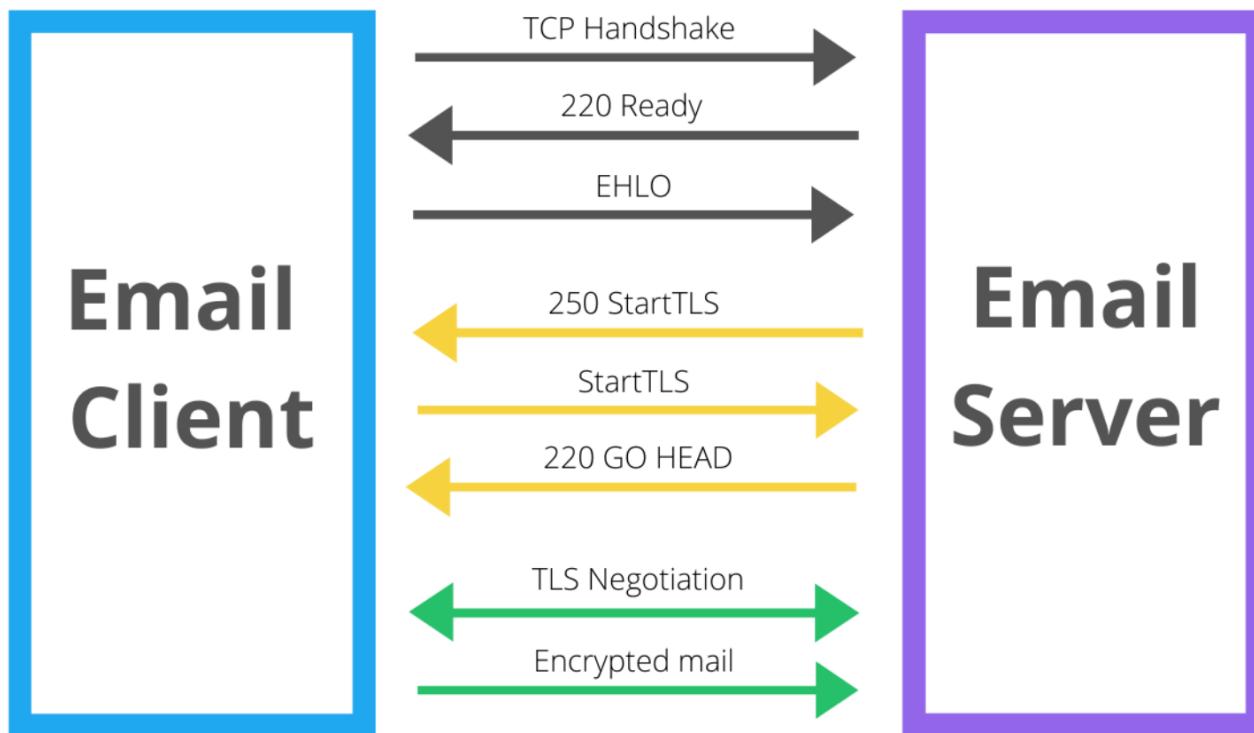
# فرمان STARTTLS

□ فرمان STARTTLS افزونه‌ای بر پروتکلهای متن آشکار است، که با اجرای آن می‌توانند یک اتصال ناامن را به اتصالی آمن 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

پست الکترونیکی

[amini@sharif.edu](mailto:amini@sharif.edu)

[kharrazi@sharif.edu](mailto:kharrazi@sharif.edu)