

یادداشت‌های امن و آسان

امنیت وب

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمد رضا رازیان*

بهار و تابستان 1395

مرکز تخصصی آفا

دانشگاه سمنان

*Homepage: www.mrazian.com



آفا دانشگاه سمنان

مرکز تخصصی آفا دانشگاه سمنان
<http://cert.semnan.ac.ir>



آزمایشگاه امنیت داده و شبکه شریف
<http://dnsl.ce.sharif.ir>



فهرست مطالب



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



خطرات تهدیدکننده وب

- با وجود سادگی راه اندازی خدمات مبتنی بر وب و گستردگی استفاده از مرورگرها، برنامه های تحت وب از پیچیدگی بالا و تهدیدات بالقوه فراوانی برخوردار است.

- نمونه ای از خطرات متداول:

- حمله به وب سرورها
- تهدید اعتبار برنامه های 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 به وب سرور
- حملات به مرورگر وب
- حملات به ترافیک شبکه وب: **موضوع بحث این جلسه**



تهدیدات در وب



آپادانشگاه سمنان

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none">•Modification of user data•Trojan horse browser•Modification of memory•Modification of message traffic in transit	<ul style="list-style-type: none">•Loss of information•Compromise of machine•Vulnerability to all other threats	Cryptographic checksums
Confidentiality	<ul style="list-style-type: none">•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	<ul style="list-style-type: none">•Loss of information•Loss of privacy	Encryption, web proxies
Denial of Service	<ul style="list-style-type: none">•Killing of user threads•Flooding machine with bogus requests•Filling up disk or memory•Isolating machine by DNS attacks	<ul style="list-style-type: none">•Disruptive•Annoying•Prevent user from getting work done	Difficult to prevent
Authentication	<ul style="list-style-type: none">•Impersonation of legitimate users•Data forgery	<ul style="list-style-type: none">•Misrepresentation of user•Belief that false information is valid	Cryptographic techniques



فهرست مطالب



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



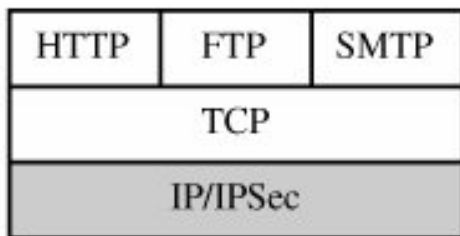
روشهای مختلف تامین امنیت وب



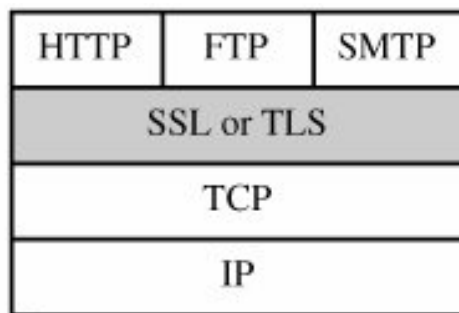
- استفاده از IPsec
 - همه منظوره
 - پنهان از دید کاربران لایه بالاتر
 - سربرار استفاده از IPsec (به خصوص در سمت کارفرما)
- استفاده از SSL/TLS
 - پنهان از دید برنامه‌های کاربردی
 - پشتیبانی مرورگرها و نیز بسیاری از وب سرورها
- سرویس‌های امنیتی وابسته به کاربرد خاص
 - تراکنش‌های مالی امن (SET)



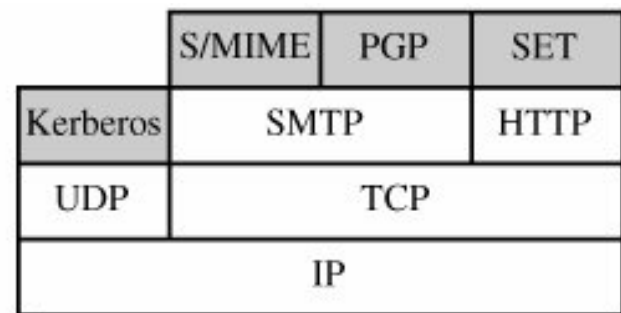
روشهای مختلف تامین امنیت وب



(a) Network level



(b) Transport level



(c) Application level



فهرست مطالب



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



SSL – معرفی

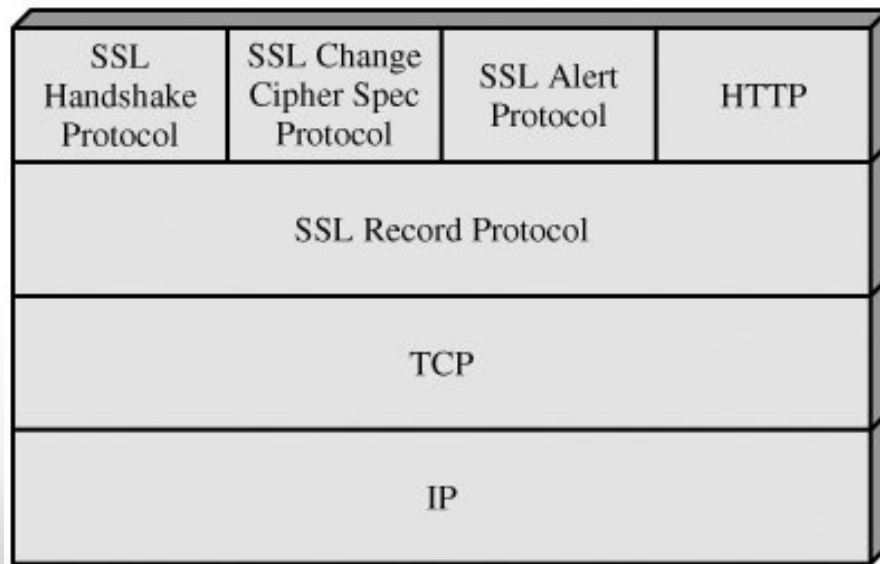


- لایه امنیتی در بالای لایه انتقال
- ارائه شده توسط شرکت Netscape و نسخه ۳ آن نسخه استاندارد اینترنت است.
- سرویس قابل اطمینان انتها به انتها (end to end) و مبتنی بر TCP
- پروتکل آن در دو لایه پیاده‌سازی می‌شود.



SSL – معماری

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





SSL – مفاهیم

- با استفاده از SSL یک نشست امن برقرار می‌شود و در طی یک نشست چند اتصال امن برقرار می‌شود.

اتصال (Connection)

- یک ارتباط همتا-به-همتای امن (رمزگذاری همراه با MAC) در لایه انتقال
- هر اتصال به یک **نشست** نگاشت 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.



فهرست مطالب



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



SSL – پروتکلها



• پروتکل SSL Record

دو سرویس برای SSL فراهم می کند:

• محرمانگی پیام

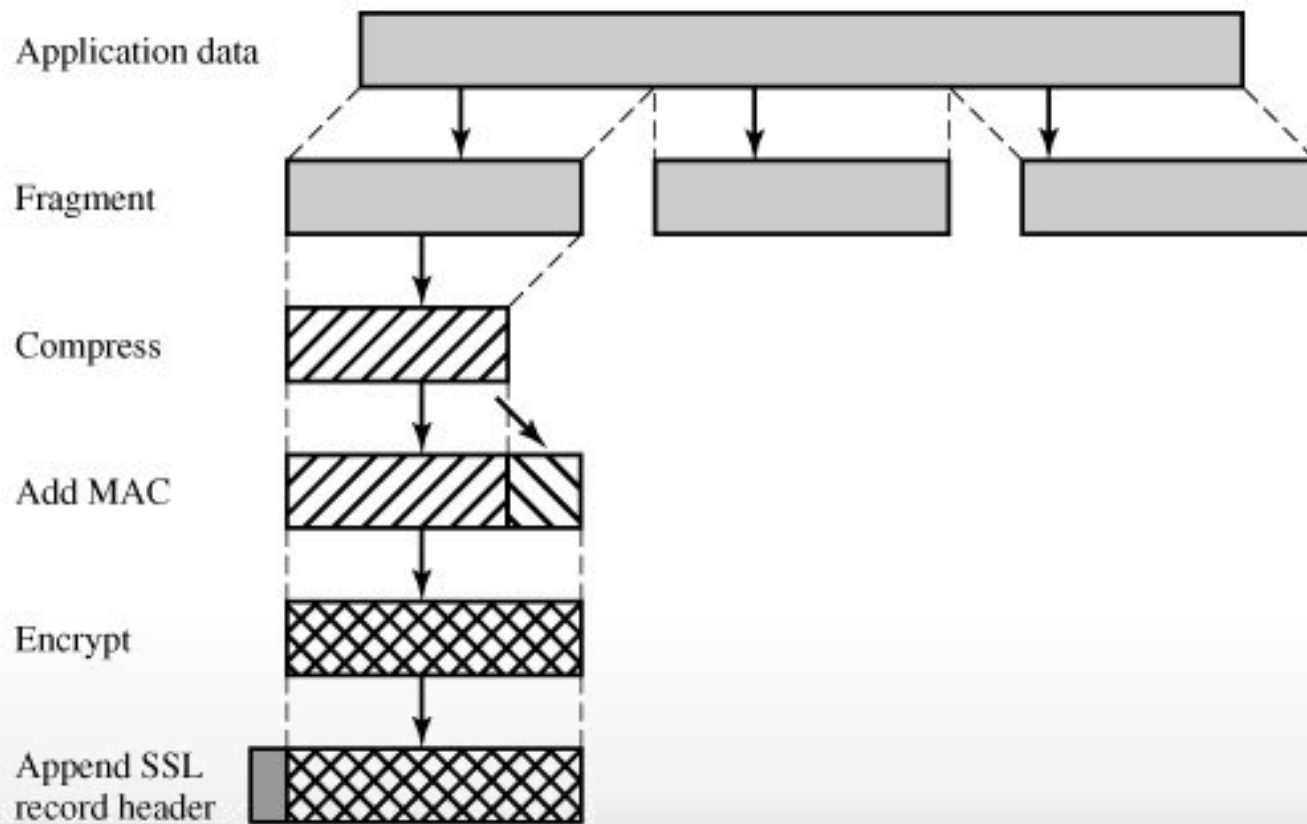
- با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به اشتراک گذاشته شده است.
- استفاده از یکی از الگوریتم‌های IDEA، RC2-40، DES-40، DES، 3DES، RC4-128، RC4-40، Fortezza

• صحت پیام

- تولید MAC با استفاده از کلید متقارن مخفی
- استفاده از SHA-1 یا MD5



اَعمال پروتکل Record



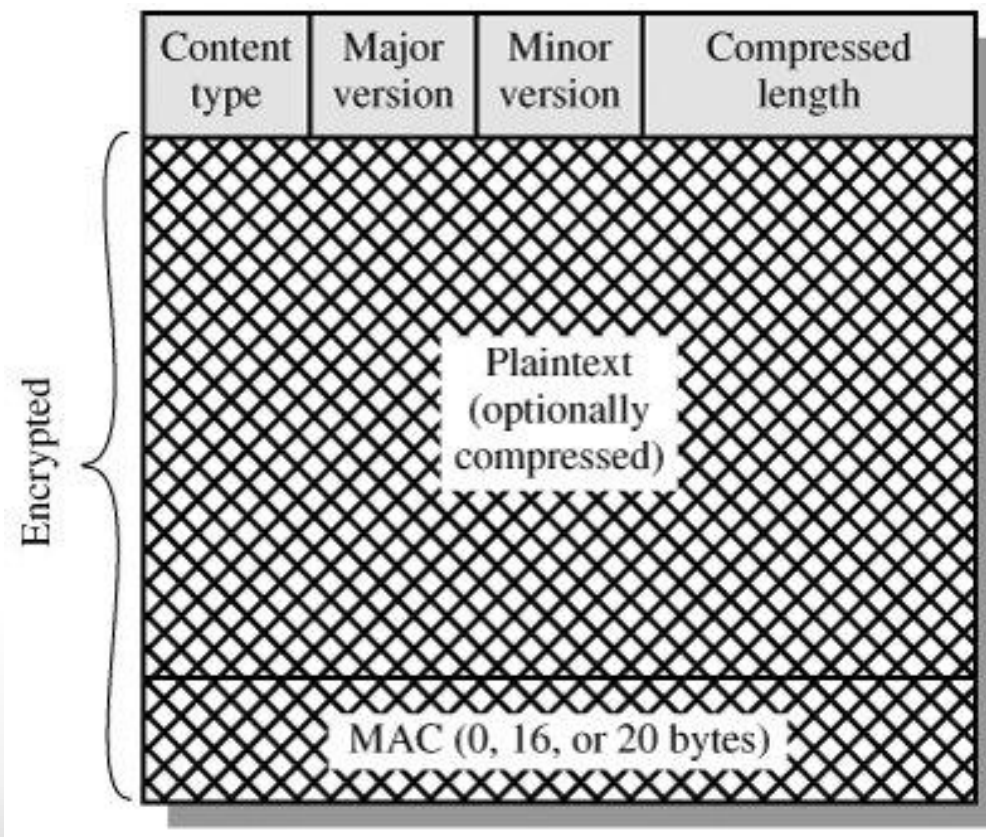


SSL – پروتکلها

- اعمال انجام شده در پروتکل 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:
 - (محتوای قطعه، طول قطعه، نوع فشرده‌سازی، شماره سریال)
 - الگوریتم درهم‌ساز مورد استفاده، MD5 یا SHA-1 است.
- رمزنگاری: استفاده از رمز قطعه‌ای یا جریانی.
- اضافه کردن سرآیند: به ابتدای قطعه رمز شده می‌چسبد و شامل عناصر زیر است:
 - (نوع محتوا، نسخه اصلی SSL، نسخه فرعی SSL، طول داده فشرده شده)
 - نوع محتوا (Content Type) بیان کننده پروتکل استفاده کننده از این سرویس در لایه بالاتر است.



قالب SSL Record





SSL – پروتکلها

• پروتکل Change Cipher Spec:

- یکی از ۳ پروتکل لایه دوم SSL که از پروتکل Record استفاده می کنند.
- شامل یک بایت است که حاوی مقدار ۱ است.
- در انتهای اجرای پروتکل handshake، منجر به جایگزینی اطلاعات (حالت) یک نشست جدید معلق (pending) به جای نشست فعلی می شود تا در اتصال جاری مورد استفاده قرار گیرد.

1 byte



(a) Change Cipher Spec Protocol



SSL – پروتکلها



• پروتکل SSL Alert:

- هشدارها و خطاهای مربوط به SSL را به طرف مقابل منتقل می کند.
- **Level**: شدت خطای پیش آمده؛ Warning یا Fatal.
- **Alert**: کد نمایانگر نوع خطا از جمله:

1 byte 1 byte

Level	Alert
-------	-------

- unexpected message, bad record mac, decompression failure, handshake failure

(b) Alert Protocol

- مانند بقیه داده های SSL فشرده سازی و رمزنگاری می شود.
- خطای Fatal موجب خاتمه یک اتصال و عدم ایجاد اتصال جدید در آن نشست می شود.



SSL – پروتکلها



• پروتکل 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.
- الگوریتم‌های رمزنگاری، توابع درهم ساز مورد استفاده و کلیدهای رمزنگاری متقارن و نامتقارن را رد و بدل 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
- پروتکلها
- **فازهای پروتکل Handshake**
- بسته پروتکل TLS



پروتکل SSL Handshake



• پروتکل SSL Handshake

- شامل ۴ فاز اصلی زیر است:
- مشخص کردن قابلیت‌های رمزنگاری 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



پروتکل 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
- پیشنهاد مکانیزم فشرده‌سازی مناسب
- انتخاب برترین الگوریتم رمزنگاری و فشرده‌سازی مورد توافق طرفین توسط کارگزار



پروتکل 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 واری می کند.
- کارفرما کلید سری را تولید کرده و رمز شده به کارگزار می فرستد.
- یا این که پارامترهای DH را ارسال می کند تا هر دو طرف کلید سری را محاسبه کنند.
- در صورت درخواست کارگزار، کارفرما گواهی کلید عمومی خود را به همراه امضای تمام پیام های ارسالی و دریافتی (برای احراز اصالت خود) به کارگزار می فرستد.



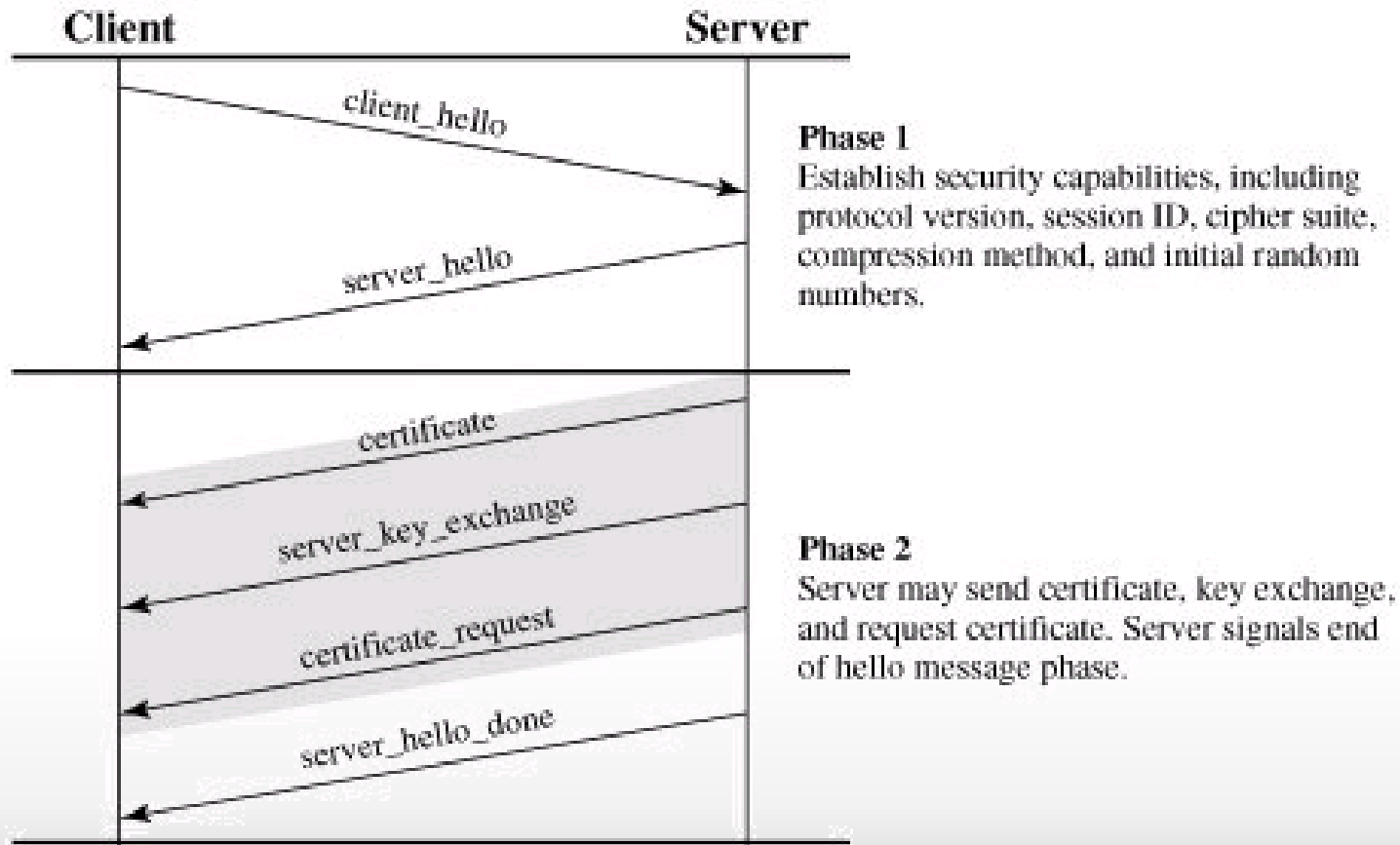
۴ – Handshake پروتکل فاز خاتمه



- فعال کردن پروتکل 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

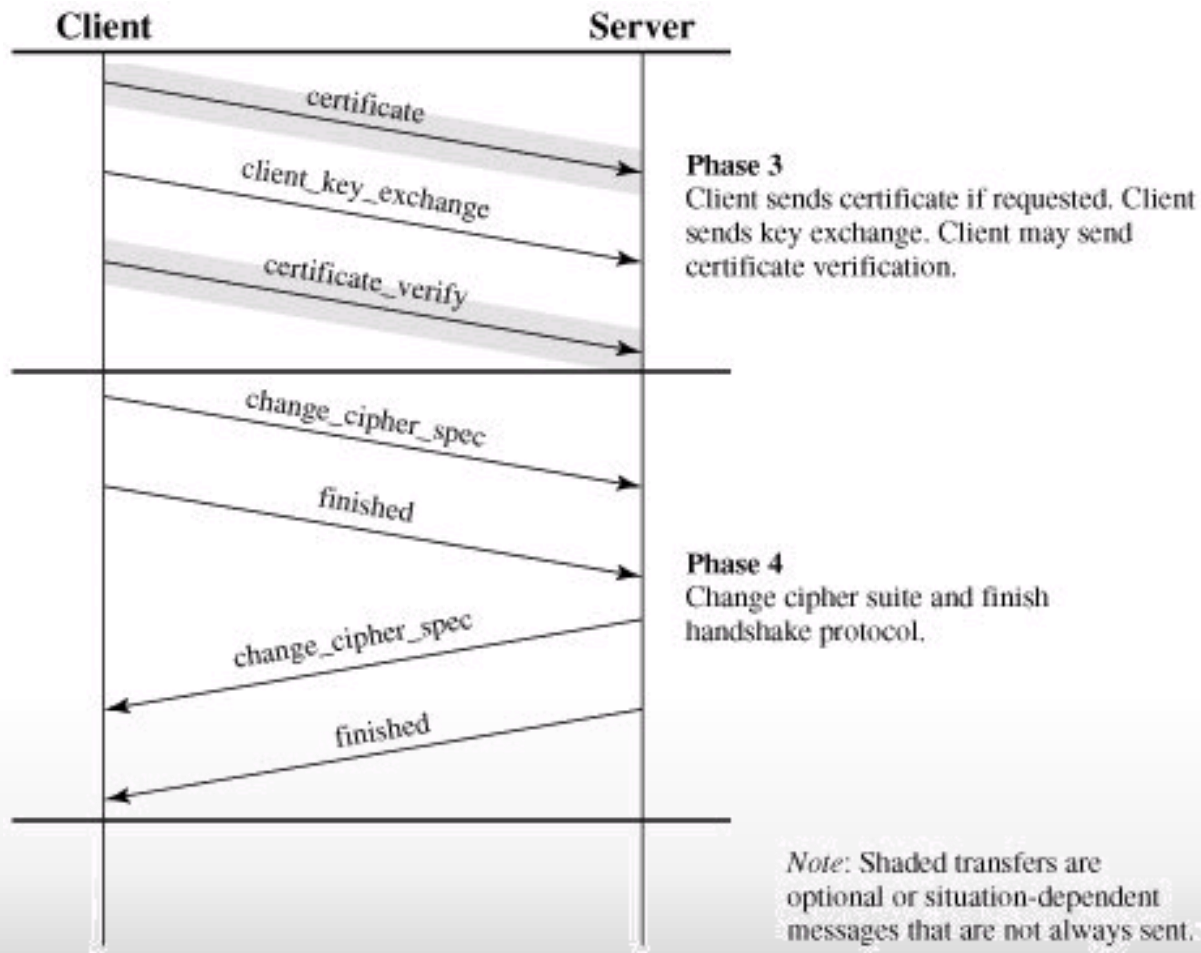


SSL Handshake پروتکل





SSL Handshake پروتکل





SSL – جمع بندی

- SSL نیازهای امنیتی زیر را فراهم می کند:
 - 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
- 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.
- بسیار شبیه SSL نسخه ۳ بدون در نظر گرفتن تفاوت‌های جزئی زیر:
 - بهره‌گیری 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.
 - ...



منابع



• اسلایدهای دکتر مرتضی امینی (منبع اصلی) - درس امنیت داده و شبکه