madsage
IRan Education
Research
NETwork
(IRERNET)

شبکه آموزشی - پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

یا ذاالامن والامان

امنیت داده و شبکه

امنیت وِب

مرتضی امینی - نیمسال اول ۹۱-۹۰

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

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 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 به وب سرور
  - حملات به 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

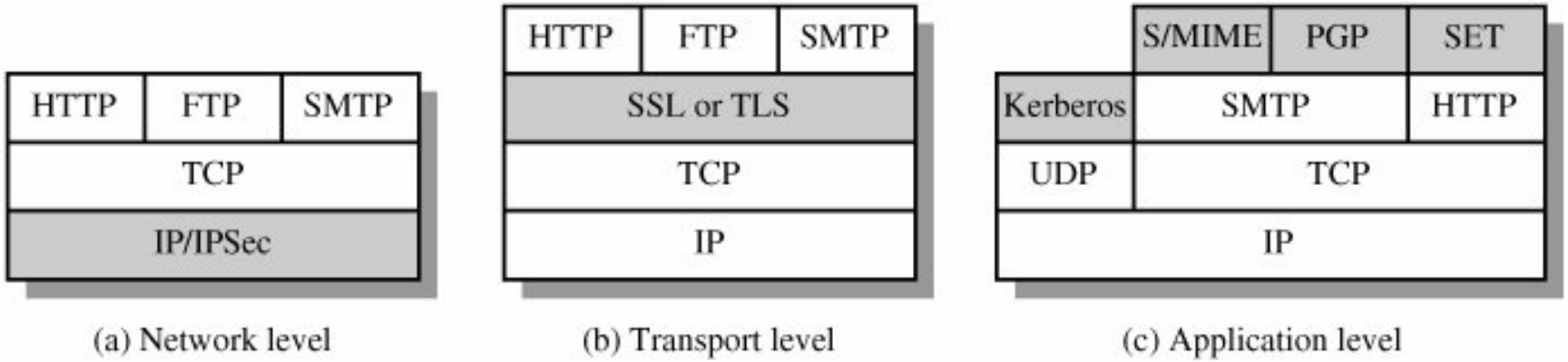
فهرست مطالب

- 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
  - 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



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 – تاریخچه

- July, 1994
  - شرکت Netscape طراحی SSL 1.0 را انجام داد.
  - این نسخه هیچ‌گاه منتشر نشد!
- Dec, 1994
  - مرورگر Netscape همراه با SSL 2.0 به بازار عرضه شد.
  - آسیب پذیر بود. کمتر از ۱ ساعت می‌شد به آن نفوذ کرد.
  - محدودیت استفاده از کلیدهای ۴۰ بیتی در خارج آمریکا

SSL – تاریخچه

- July, 1995
  - مایکروسافت نسخه جدیدی از IE را به بازار عرضه کرد که از SSL پشتیبانی می‌کرد.
  - پشتیبانی از مدهای کاری جدید و افزایش طول کلیدهای قابل استفاده
- Nov, 1995
  - شرکت Netscape توصیف SSL 3.0 را منتشر کرد.
  - با تغییرات و جهش عمده نسبت به نسخه‌های قبلی همراه بود.
  - ضمن اینکه نسبت به نسخه SSL v2.0، Backward Compatible بود.

SSL – تاریخچه

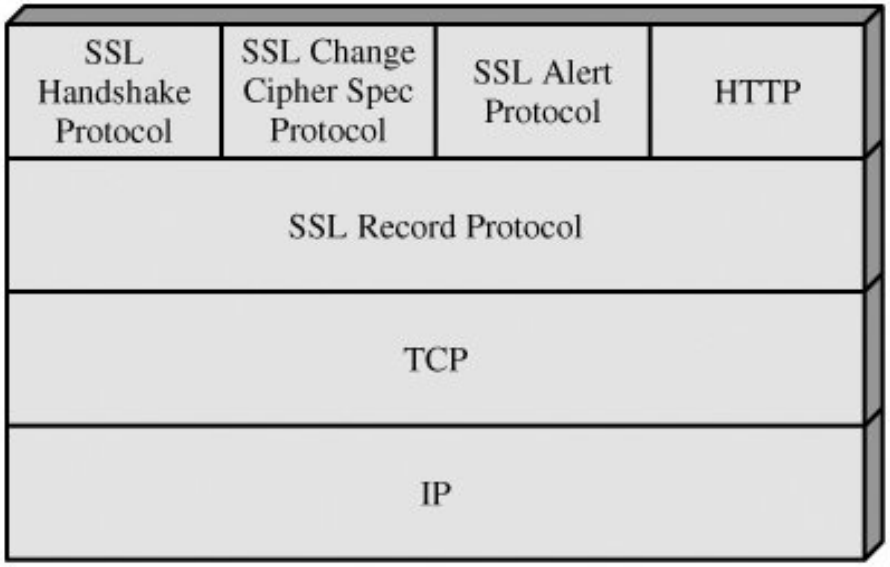
- May, 1996
  - IETF گروه کاری TLS را تشکیل داد و مسئولیت پاسخگویی به مشکلات قرارداد SSL را برعهده گرفت.
- Jan, 1999
  - TLS 1.0 بطور رسمی همراه با RFC 2246 به بازار عرضه شد.
  - در واقع همان SSL v3.1 بود که به دلایل تجاری تغییر نام داده بود.

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

- 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

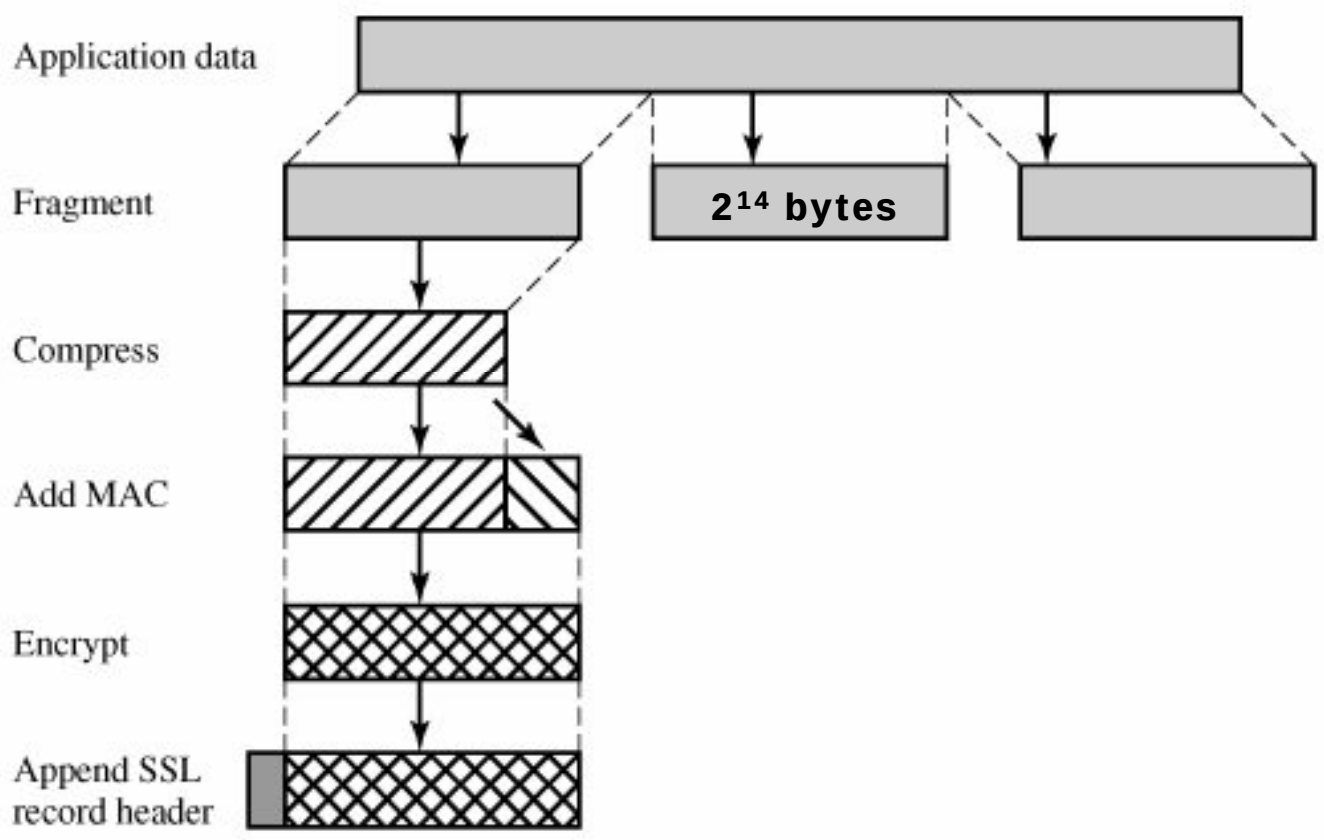
SSL – پروتکلها

پروتکل SSL Record

دو سرویس برای SSL فراهم می‌کند:

- 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، Fortezza، RC4-40، RC4-128
- صحت پیام
  - تولید MAC با استفاده از کلید متقارن مخفی
  - استفاده از SHA-1 یا MD5

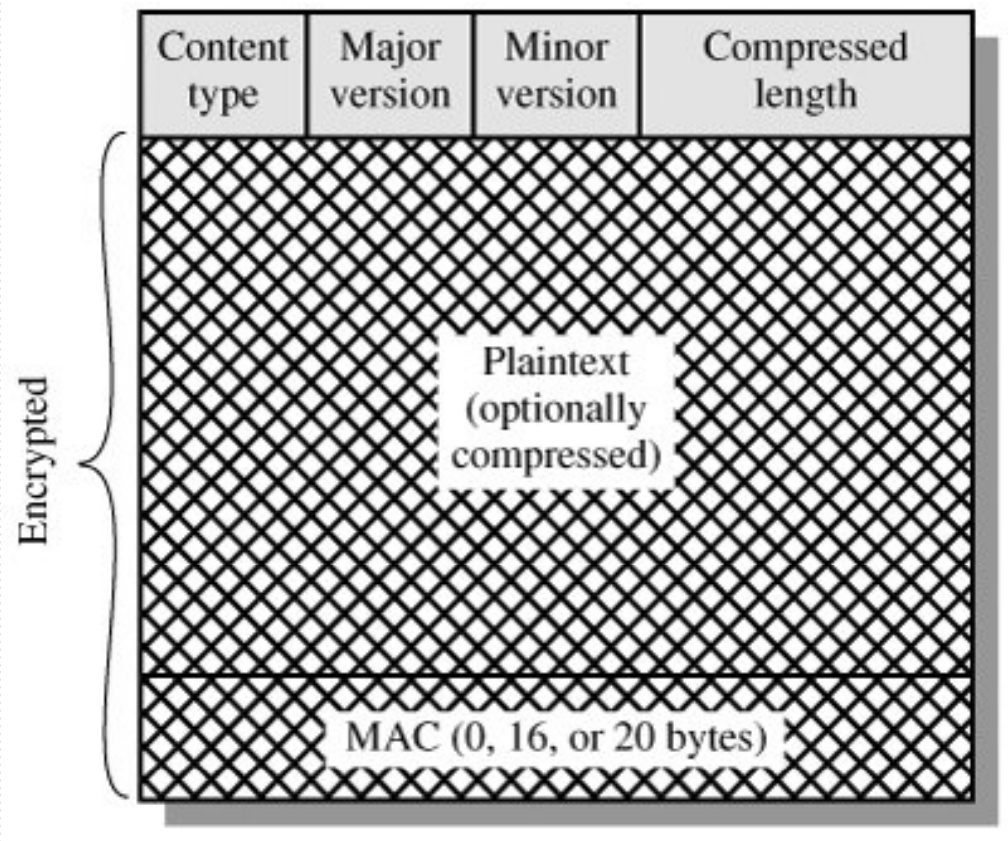
اَعمال پروتکل Record



SSL – پروتکلها

- اعمال انجام شده در پروتکل Record
  - قطعه‌بندی: تولید قطعاتی به طول $۲^{۱۴}$ یا کمتر .
  - فشرده‌سازی: اختیاری و بدون از دست رفتن داده.
  - تولید MAC: مشابه HMAC و روی ورودی زیر انجام می گیرد:
    - (محتوای قطعه، طول قطعه، نوع فشرده‌سازی، شماره سریال)
    - الگوریتم درهم‌ساز مورد استفاده، MD5 یا SHA-1 است.
  - رمزنگاری: استفاده از رمز قطعه‌ای یا جریانی.
  - اضافه‌کردن سرآیند: به ابتدای قطعه رمزشده 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 می‌کنند.
- شامل یک بایت است که حاوی مقدار ۱ است.
- در انتهای اجرای پروتکل handshake، منجر به جایگزینی اطلاعات (حالت) یک نشست جدیدِ معلق (pending) به جای نشست فعلی می‌شود تا در اتصال جاری مورد استفاده قرار گیرد.

(a) Change Cipher Spec Protocol

SSL – پروتکلها

- پروتکل 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

1 byte	1 byte
Level	Alert

(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 – 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.

1 byte	3 bytes	≥ 0 bytes
Type	Length	Content

(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 فشرده سازی مورد توافق طرفین توسط کارگزار

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

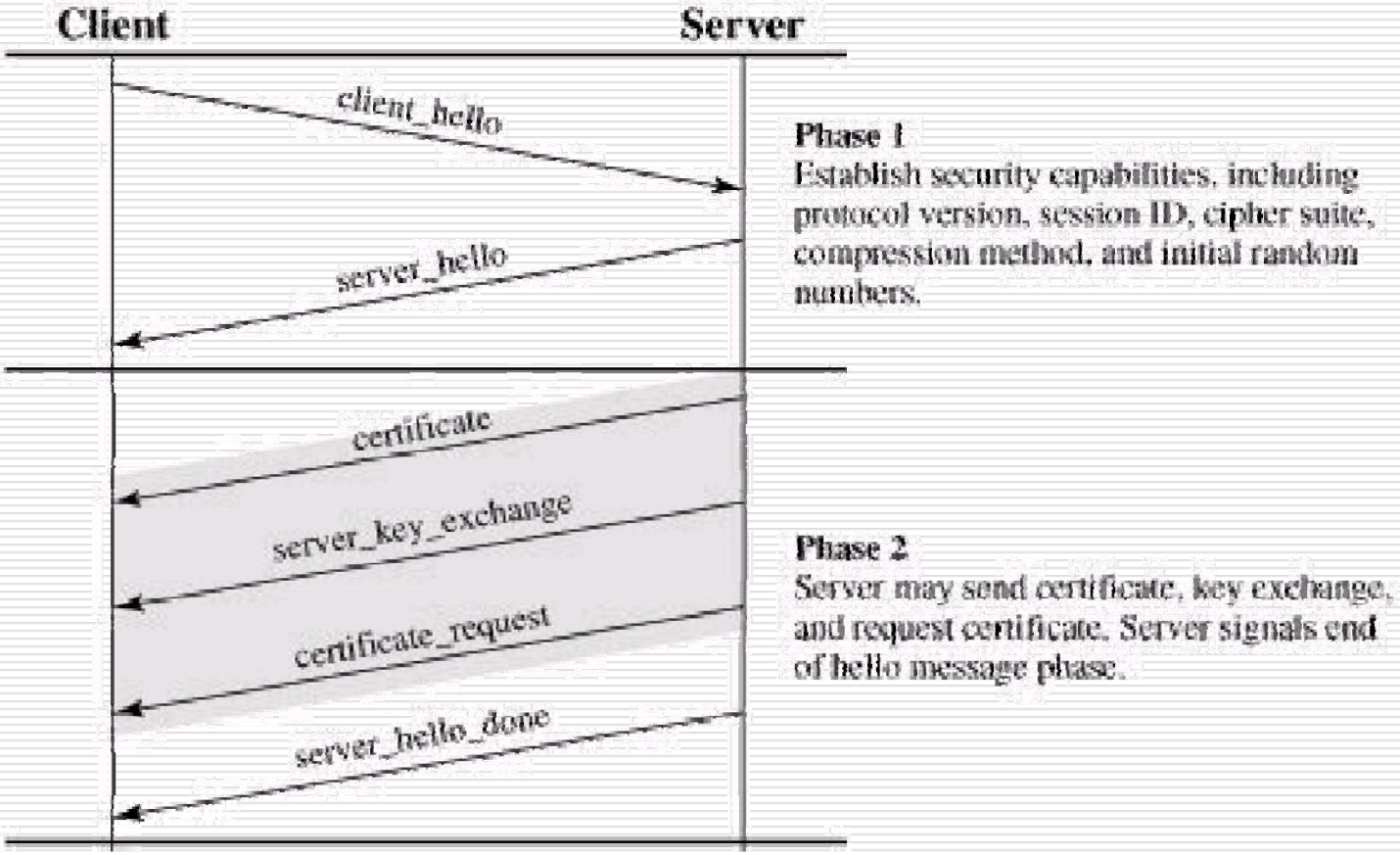
- ارسال گواهی کارگزار برای کارفرما
  - همراه با کلید عمومی (RSA) یا پارامترهای DH
- تولید و ارسال کلید سری
  - کارفرما گواهی کلید عمومی کارگزار را وارسی می‌کند.
  - کارفرما کلید سری را تولید کرده و رمزشده به کارگزار می‌فرستد.
  - یا این که هر دو با استفاده از پارامترهای DH کلید سری را محاسبه می‌کنند.
  - 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.

پروتکل Handshake – ۴
فاز خاتمه

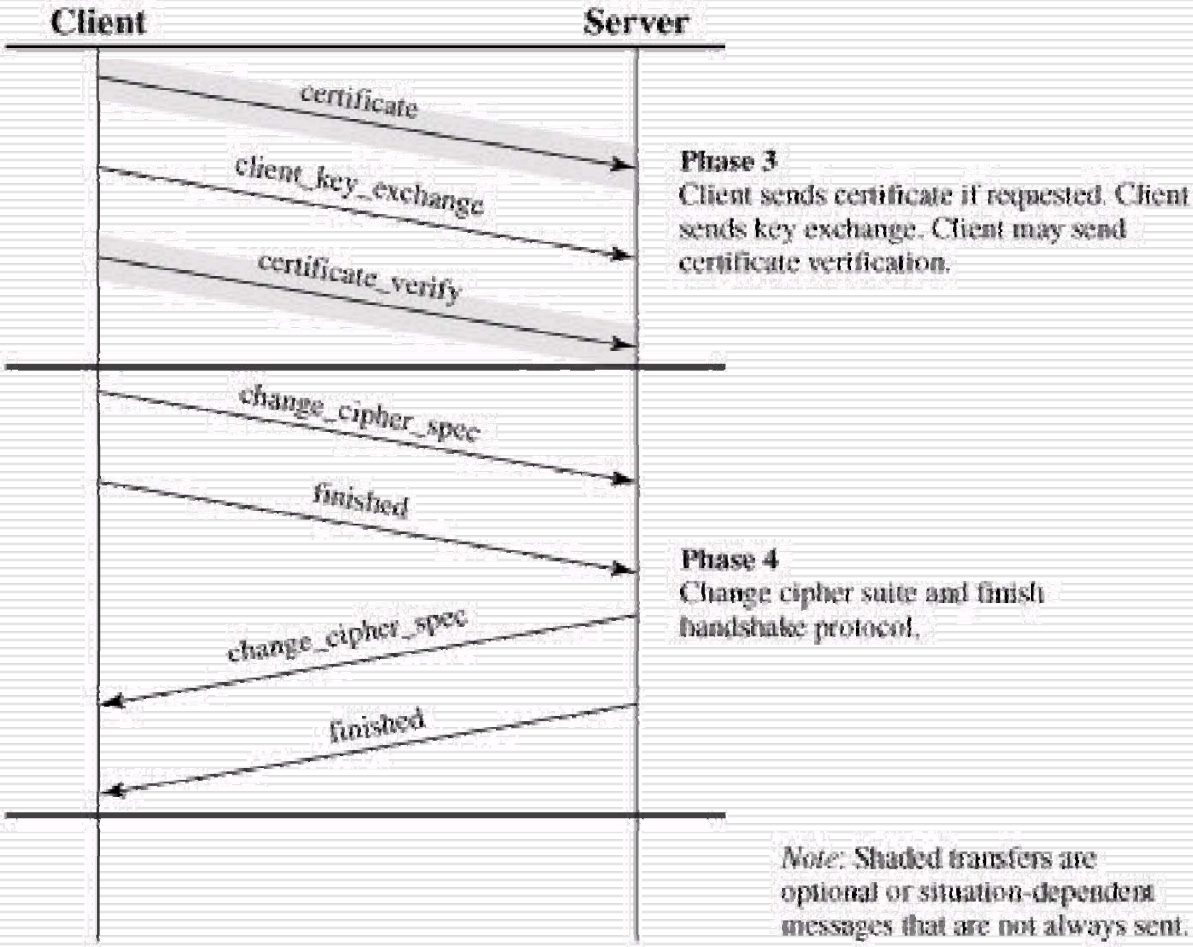
- فعال کردن پروتکل تغییر مشخصات رمز (Change Cipher Spec)
  - کارفرما پیام پروتکل تغییر مشخصات رمز را برای کارگزار می‌فرستد.
  - کارگزار حالت خود را بروز کرده (با پارامترهای توافق شده در پروتکل Handshake) و پیام پروتکل تغییر مشخصات رمز را برای کارفرما ارسال می‌کند.

- 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

پروتکل SSL Handshake



پروتکل SSL Handshake



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
- 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 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.
  - . . .

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu