دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

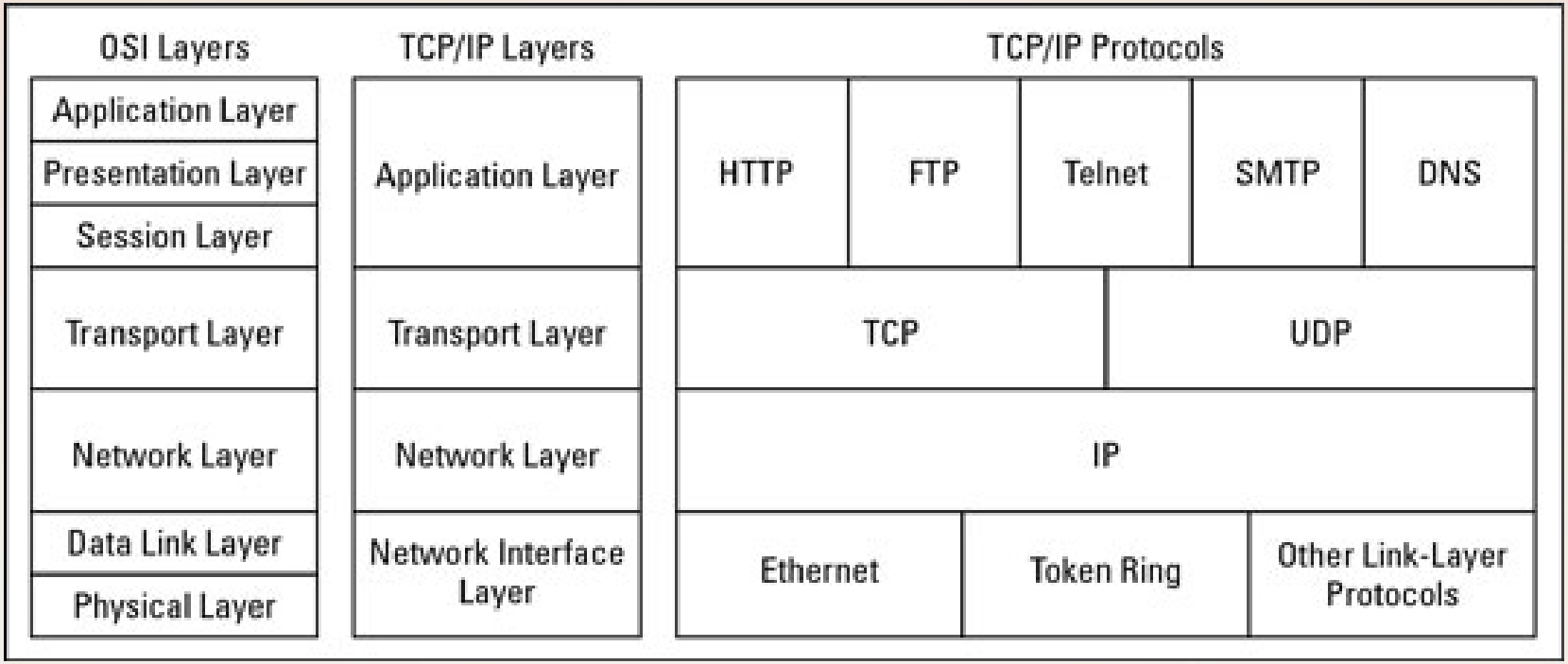
SSL

نستوه طاهری جوان

nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- یادآوری: معماری لایه ای در اینترنت



nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- ✓ یادآوری: مولفه های امنیتی مرور شده

  - Confidentiality
  - Data Integrity
  - Non-Repudiation
  - Authentication

nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- ✓ یادآوری: رویکردها
  - ○ امنیت انتها به انتها در سطح برنامه کاربردی
    - • رمزنگاری در برنامه های کاربردی، مانند PGP و SET
  - ○ امنیت انتها به انتها در سطح لایهٔ انتقال
    - • مزیت: درگیر نشدن برنامه های کاربردی، مانند TLS و SSL
  - ○ امنیت در لایهٔ شبکه
    - • انجام رمزنگاری و احراز هویت در لایهٔ شبکه، مانند IPsec
  - ○ امنیت در لایهٔ پیوند داده
    - • رمزنگاری در سطح فریم ها، مانند WPA و WEP ،L2TP
  - ○ امنیت در لایهٔ فیزیکی
    - • استفاده از محافظت های فیزیکی در شبکه های سیمی یا چنل-هاپینگ در بیسیم

nastooh@aut.ac.ir

SSL

- ✓ پروتکل SSL (Secure Socket Layer)
  - نکته: در کاربردهای تجاری، نمیتوان فقط به امنیت لایهٔ شبکه اتکا کرد.
    - نیاز به برقراری امنیت در لایهٔ کاربرد، یا حداقل در لایهٔ انتقال داریم!!!
    - یعنی امنیت انتها-به-انتها
  - SSL در انتهای دههٔ ۹۰ میلادی توسط شرکت نت اسکیپ پیشنهاد شد.
  - یادآوری: برنامه های کاربردی، در حالت عادی به کمک TCP یک اتصال برقرار می کنند.
    - در صورت نیاز به اتصال امن، باید از طریق SSL سوکت را برقرار کرد.

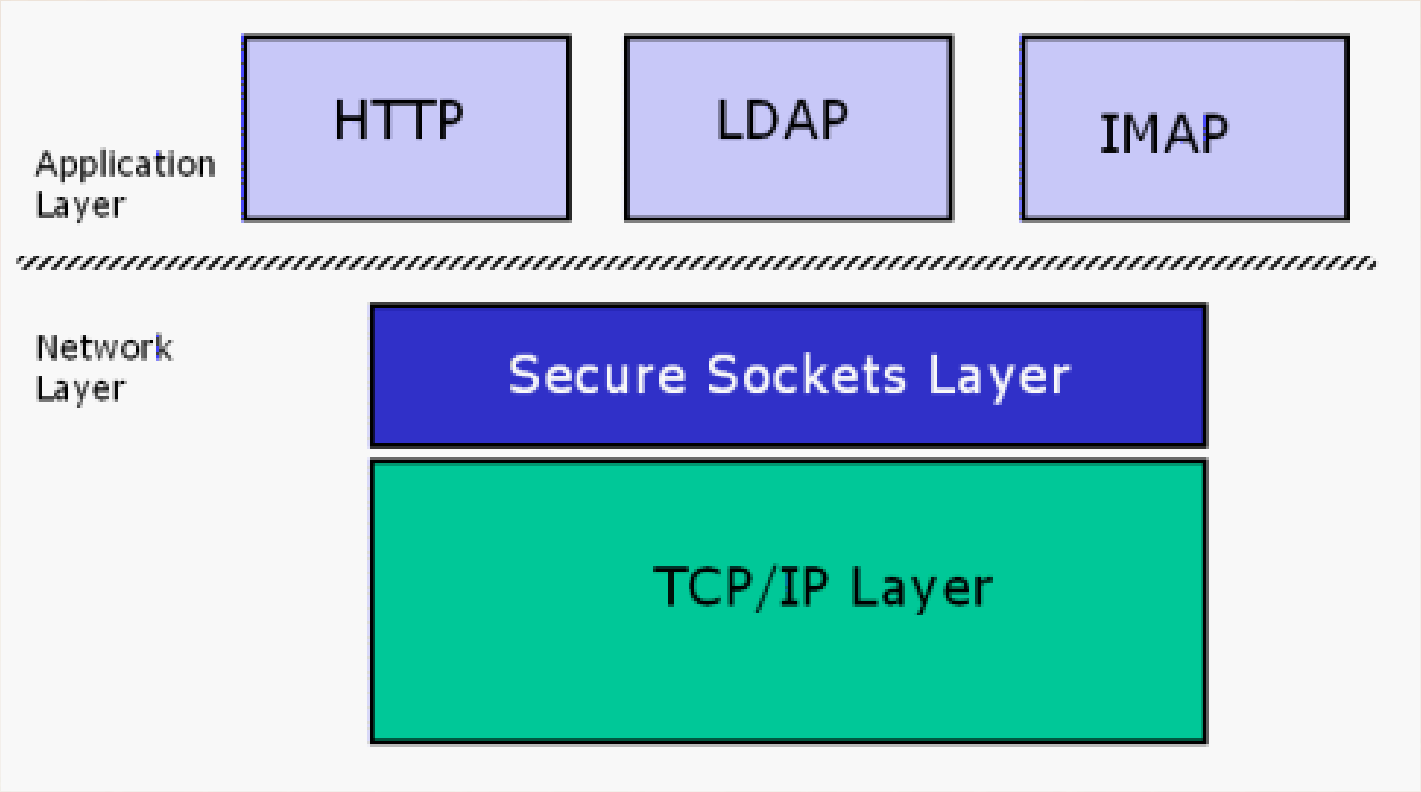
nastooh@aut.ac.ir

SSL

- ✓ پروتکل SSL
  - ○ خدمات SSL
    - مذاکره برای پارامترها و شیوه های امنیتی
    - احراز هویت نقاط انتهایی ارتباط
    - تبادل اطلاعات به صورت رمزشده
    - بررسی صحت و اصالت داده ها
    - حتی فشرده سازی داده ها (اختیاری)

SSL

- پروتکل SSL
  - جایگاه پروتکل SSL



nastooh@aut.ac.ir

SSL

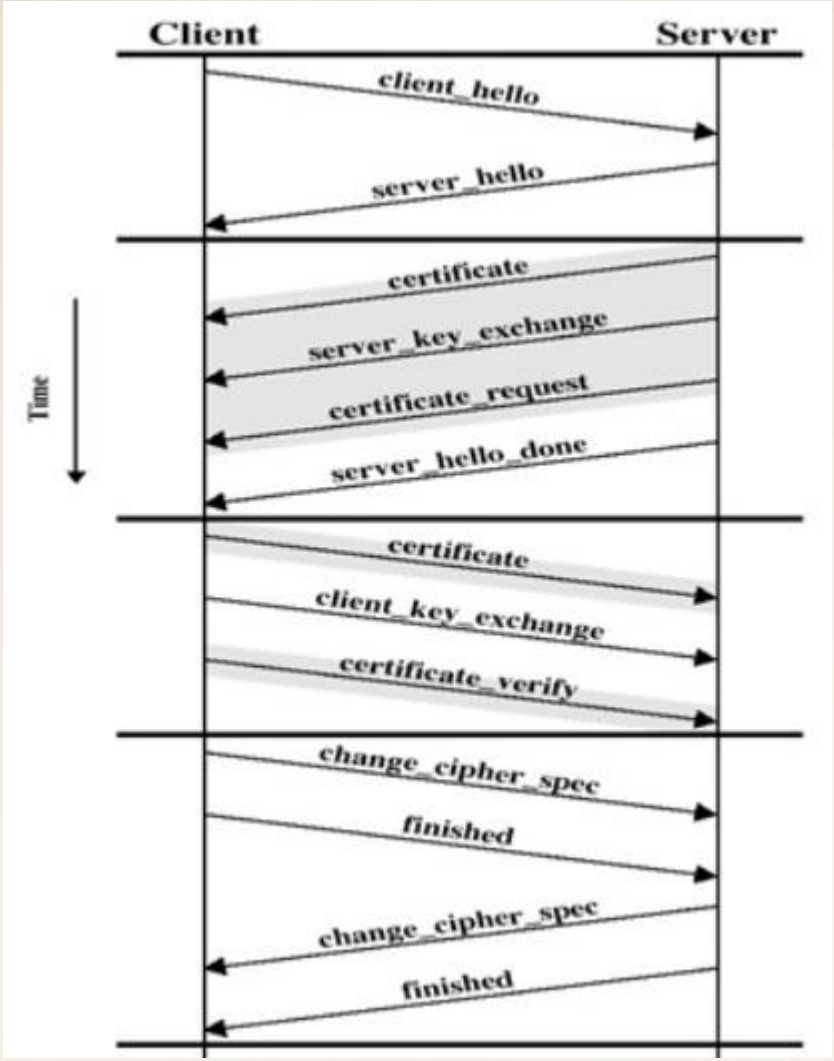
- پروتکل SSL
  - هدف اولیهٔ SSL برقراری امنیت در وب بود.
  - هنگامی که HTTP را بر روی SSL بکار بریم، آن را **HTTPS** گوییم.
  - TLS، در واقع نسخهٔ استاندارد شدهٔ SSL توسط IETF است.
    - Transport Layer Security (TLS)
  - علاوه بر HTTP، پروتکل های دیگری نظیر FTP، POP3، IMAP و Telnet قادرند بر روی SSL کار کنند.

nastooh@aut.ac.ir

SSL

- ✓ پروتکل SSL
  - روال اجرایی SSL
    - فاز اول: دست تکانی
      - هدف: مذاکره بر سر گزینه های امنیتی و ست کردن کلید.
    - فاز دوم: ارسال داده
    - فاز سوم: هشدار (برای شرایط نامتعارف، مثلا عدم اعتبار گواهی نامه ها)

SSL

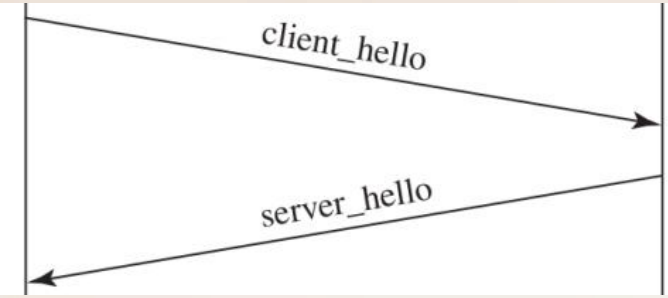


- ✓ پروتکل SSL
  - مراحل دست تکانی

nastooh@aut.ac.ir

SSL

- ✓ پروتکل SSL
  - ○ دست تکانی
    - گام اول



➢ هدف: توافق بر سر پارامترها و ورژن ها

➢ ارسال بسته سلام از جانب مشتری

« فیلدهای مهم: نسخه SSL، Session ID، لیست الگوریتم های رمزنگاری قابل استفاده، یک عدد تصادفی

➢ ارسال پاسخ بستهٔ سلام از جانب سرور

« فیلدهای مهم: تایید نسخهٔ SSL، شناسهٔ جلسه، انتخاب روش رمزنگاری از بین لیست مشتری (یک روش متقارن برای تبادل اطلاعات و یک روش نامتقارن برای ست کردن کلید)...

nastooh@aut.ac.ir

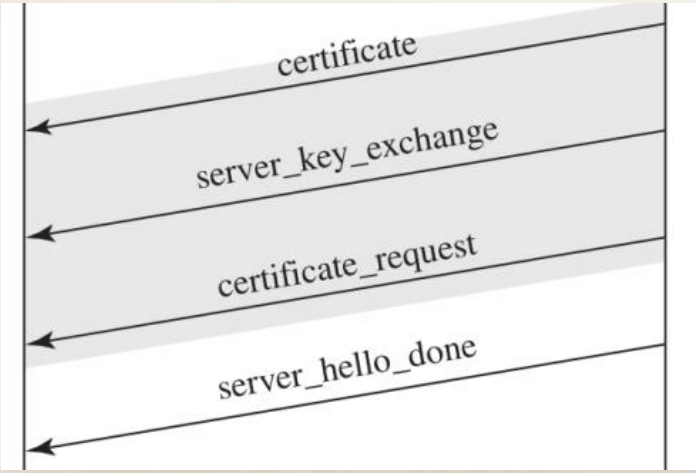
SSL

- ✓ پروتکل SSL
  - ○ دست تکانی
    - گام دوم

➢ هدف: ارسال گواهینامه سرور (اختیاری)، پیشنهاد کلید (اختیاری)، درخواست گواهینامه مشتری (اختیاری)، اعلام پایان سلام و علیک!

« در صورت نیاز گواهینامه سرور و زنجیرهٔ اعتماد ارسال می شود.

« پیشنهاد کلید از سمت سرور معمولا صورت نمی پذیرد.



nastooh@aut.ac.ir

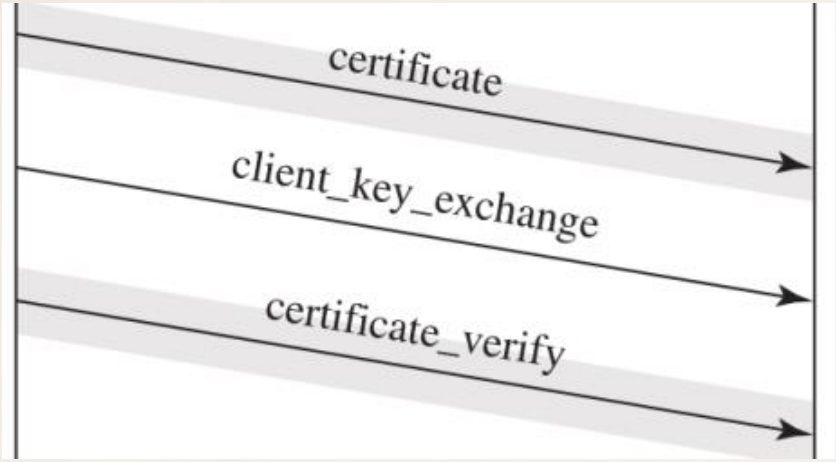
SSL

- ✓ پروتکل SSL
  - ○ دست تکانی
    - گام سوم

➢ هدف: پیشنهاد کلید از سمت مشتری، ارسال گواهینامه مشتری (اختیاری)، ارسال تاییدیه گواهینامه سرور (کاملا اختیاری)

« مشتری کلید پیشنهادی را با کلید عمومی سرور رمز می کند.

« این کلید برای رمزنگاری استفاده خواهد شد

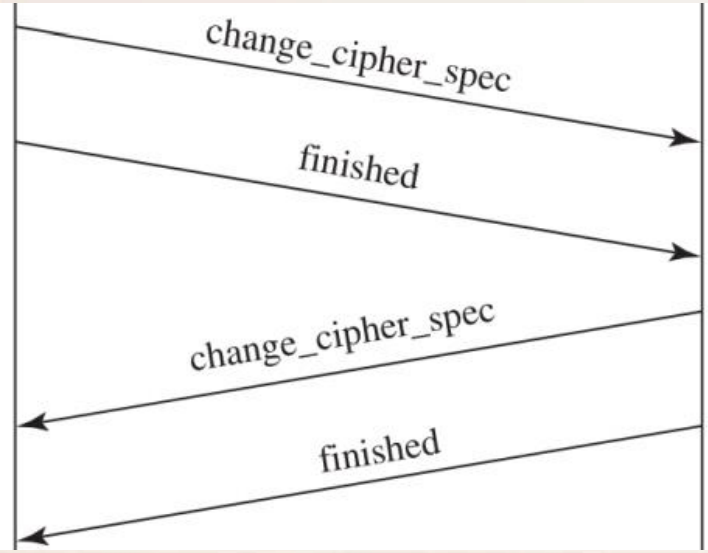


SSL

- پروتکل SSL
  - دست تکانی
    - گام چهارم

➢ هدف: تعیین جزئیات روش رمزنگاری و استفاده از رمزنگاری توافق شده

« در واقع مشتری و سرور تائید و توافق می کنند که از این به بعد از روش رمزنگاری فیکس شده و با چه جزئیاتی استفاده کنند.



nastooh@aut.ac.ir

SSL

- ✓ پروتکل SSL
  - ○ ارسال داده

- دادهٔ برنامه کاربردی به قطعاتی (با اندازه ۱۶ کیلوبایت یا کمتر) شکسته می شود.
- در صورت نیاز (توافق) میتوان قطعات را فشرده سازی هم کرد. (عموما صرف نظر)
- اضافه کردن کد MAC به انتهای داده (برای حفظ اصالت و صحت داده)
- رمزنگاری قطعه داده با روش توافق شده (مثلا DES یا AES)
- افزوده یک سرآیند به قطعه (مثلا طول داده یا شماره نسخه)
- ارسال داده از طریق TCP

- مقصد نیز پس از دریافت قطعه، صحت داده را چک کرده و آن را رمزگشایی می کند.

nastooh@aut.ac.ir

SSL

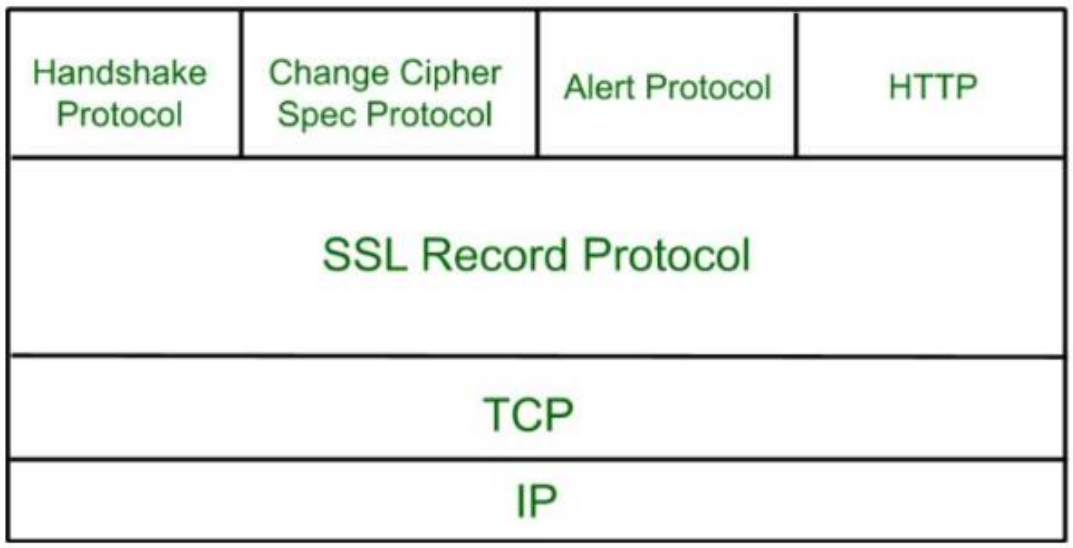
✓ پروتکل SSL

○ ارسال هشدار

- در صورتی که هر یک از طرفین نیاز بدانند، میتوانند برای هم پیام های هشدار ارسال کنند. شامل:
  - ➢ پیام در سطح Warning
  - ➢ پیام در سطح Fatal (موجب قطع ارتباط می شود)
- سطح هشدار را فرستنده مشخص می کند.
- مثال هایی از هشدارها:
  - ➢ مشکل در بررسی اصالت (MAC) یک پیام
  - ➢ دریافت پیامی غیر منتظره!
  - ➢ بروز مشکل در فرآیند دست تکانی
  - ➢ عدم اعتبار زنجیرهٔ اعتماد گواهینامه
  - ➢ دریافت گواهینامه منقضی شده

SSL

- ✓ جمع بندی پروتکل SSL
  - ○ اجزای اصلی پروتکل SSL
    - Handshake Protocol (تبادل و توافق پارامترها)
    - Change Cipher Spec Protocol (میتواند بخشی از دست تکانی باشد)
    - Alert Protocol (تبادل پیام های هشدار)
    - Record Protocol (عملیات آماده سازی داده برای اسال)



nastooh@aut.ac.ir

TLS

- TLS ✓
  - نسخهٔ استاندارد شدهٔ SSL
  - در سال ۱۹۹۹ توسط IETF استاندارد شد
  - در سند RFC2246

Protocol	Published
SSL 1.0	Unpublished
SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.1	2006
TLS 1.2	2008
TLS 1.3	2018

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir