به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

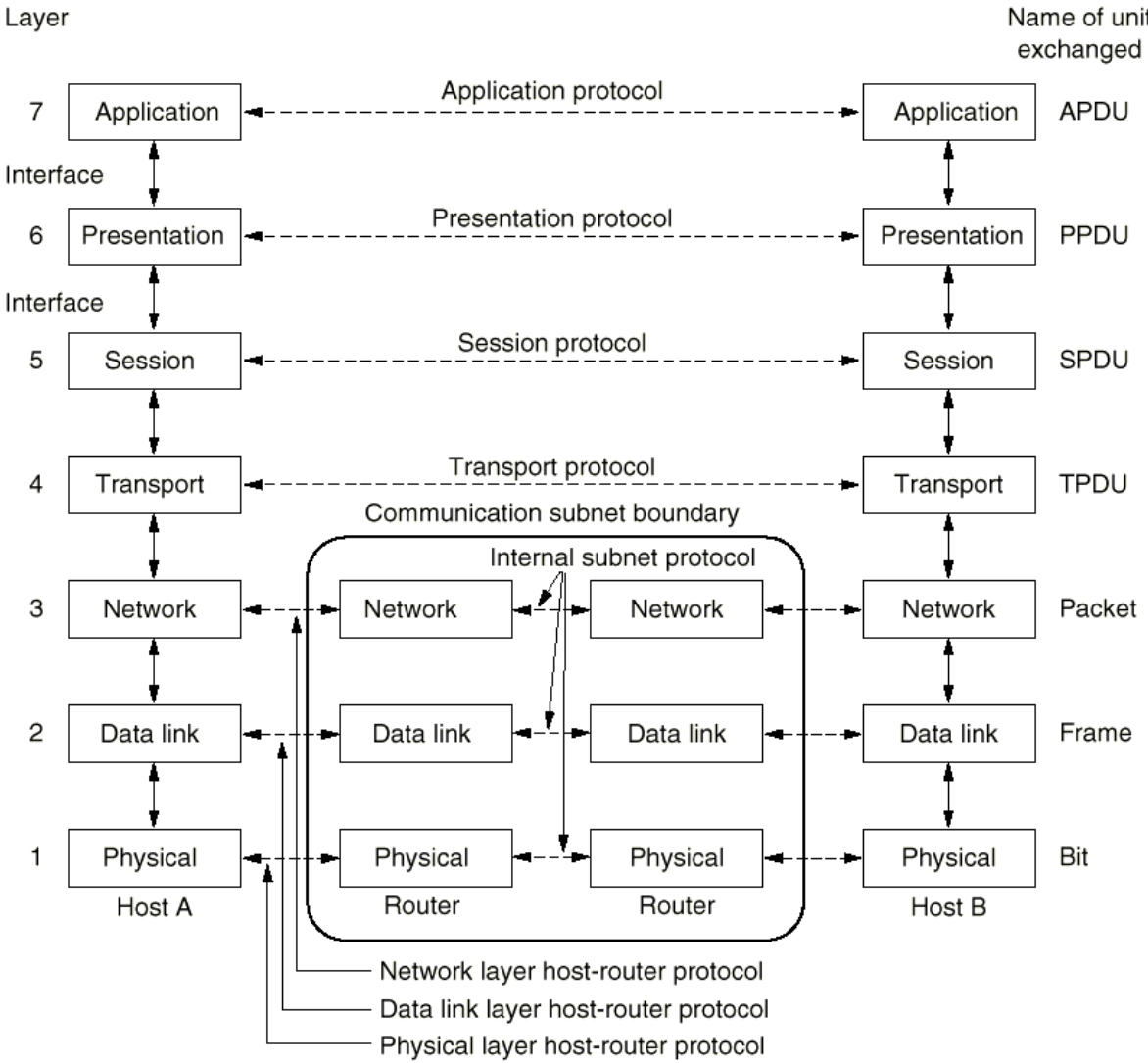
امنیت وب
(در سطح لایه انتقال)

Web Security
(Transport-Level Security)

مهتاب میرمحسنی

نیم‌سال دوم (بهار) ۹۸-۹۹

مدل OSI (Open System Interconnection)



- ۷ لایه
  - هر لایه چه کاری را انجام می‌دهد (و نه چگونه)

۱- لایه فیزیکی

۲- لایه پیوند داده‌ها

۳- لایه شبکه

۴- لایه انتقال

۵- لایه نشست

۶- لایه ارائه (نمایش)

۷- لایه کاربرد

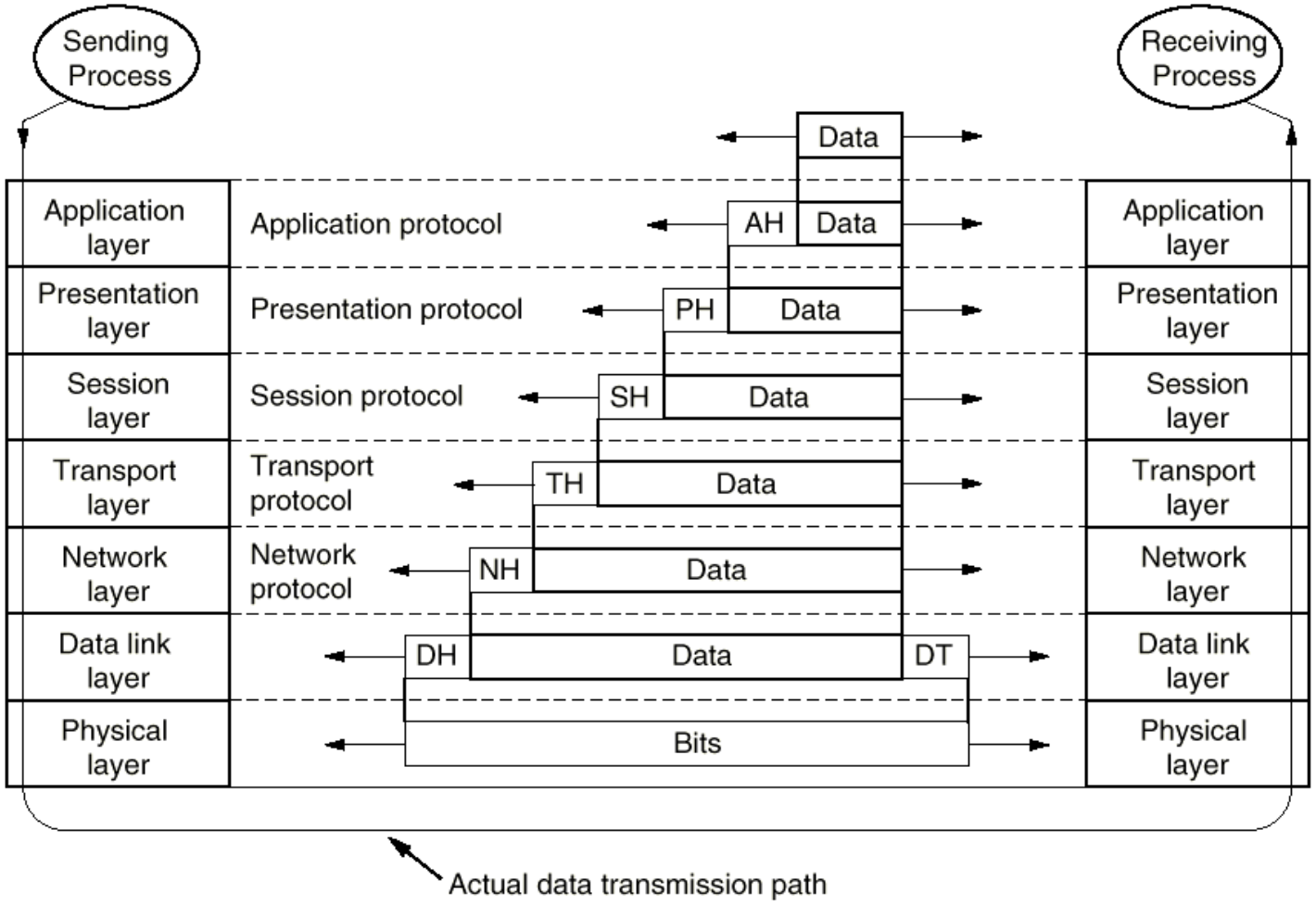
مدل OSI

- لایه فیزیکی
  - انتقال بیت ها به صورت سیگنال الکتریکی و ارسال آن بر روی کانال
  - استانداردهای انتقال: RS-232, RS-422
- لایه پیوند داده‌ها (Data link layer)
  - ارسال فریم‌ها
  - ارسال مطمئن (کشف و تصحیح خطا)
  - کنترل شار
  - پروتکل‌های معروف: SDLC و HDLC
- لایه شبکه
  - ارسال بسته‌ها (packet)
  - مسیریابی و کنترل ازدحام (Congestion)

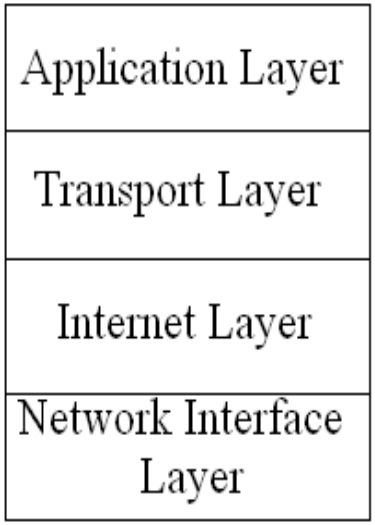
مدل OSI

- لایه فیزیکی
  - انتقال بیت ها به صورت سیگنال الکتریکی و ارسال آن بر روی کانال
  - استانداردهای انتقال: RS-232, RS-422
- لایه پیوند داده‌ها (Data link layer)
  - ارسال فریم‌ها
  - ارسال مطمئن (کشف و تصحیح خطا)
  - کنترل شار
  - پروتکل‌های معروف: SDLC و HDLC
- لایه شبکه
  - ارسال بسته‌ها (packet)
  - مسیریابی و کنترل ازدحام (Congestion)
- لایه انتقال
  - مدیریت اتصال
  - لایه انتها-به-انتها (از منبع به مقصد)
  - تقسیم دنباله پیام به بسته‌ها
  - کنترل شار
- لایه نشست: مدیریت نشست
  - ورود به سیستم از راه دور، احراز اصالت طرفین، احراز اصالت پیام‌ها، اتمام نشست، حسابداری کارخواه‌ها
- لایه ارائه(نمایش)
  - فشرده سازی، رمزنگاری، تبدیل اطلاعات به کدهای ASCII , Unicode
- لایه کاربرد: پروتکل‌های کاربردی معمول
  - مانند FTP، E-mail و ...

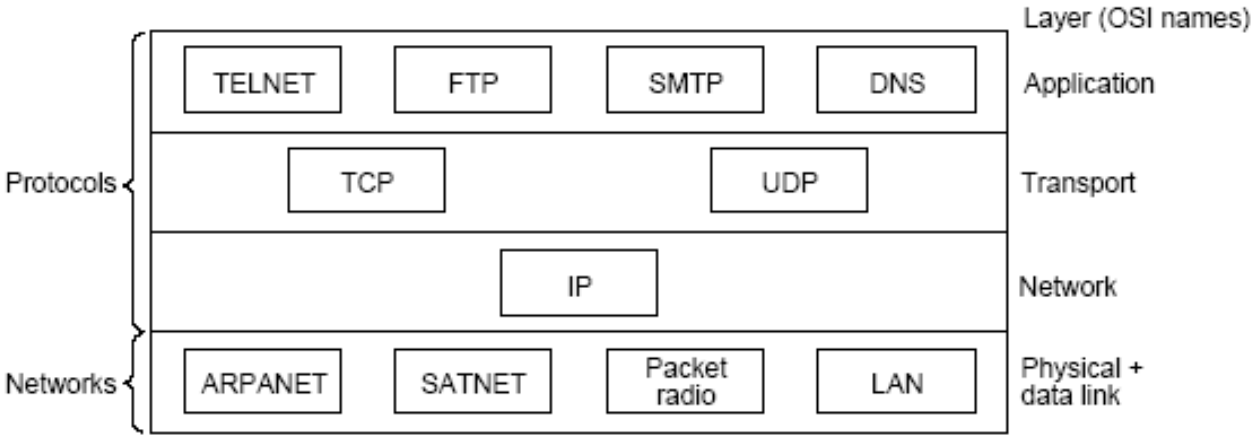
مدل OSI


Sending Process
Receiving Process
Data
Application layer
Application protocol
AH
Data
Application layer
Presentation layer
Presentation protocol
PH
Data
Presentation layer
Session layer
Session protocol
SH
Data
Session layer
Transport layer
Transport protocol
TH
Data
Transport layer
Network layer
Network protocol
NH
Data
Network layer
Data link layer
DH
Data
DT
Data link layer
Physical layer
Bits
Physical layer
Actual data transmission path

مدل TCP / IP



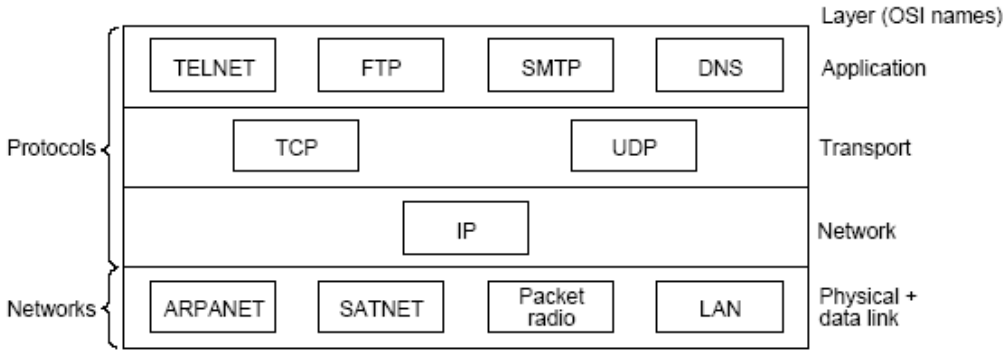
- توسط ARPA NET
- لایه واسط شبکه
- لایه اینترنت (شبکه)
- لایه انتقال
- لایه کاربرد



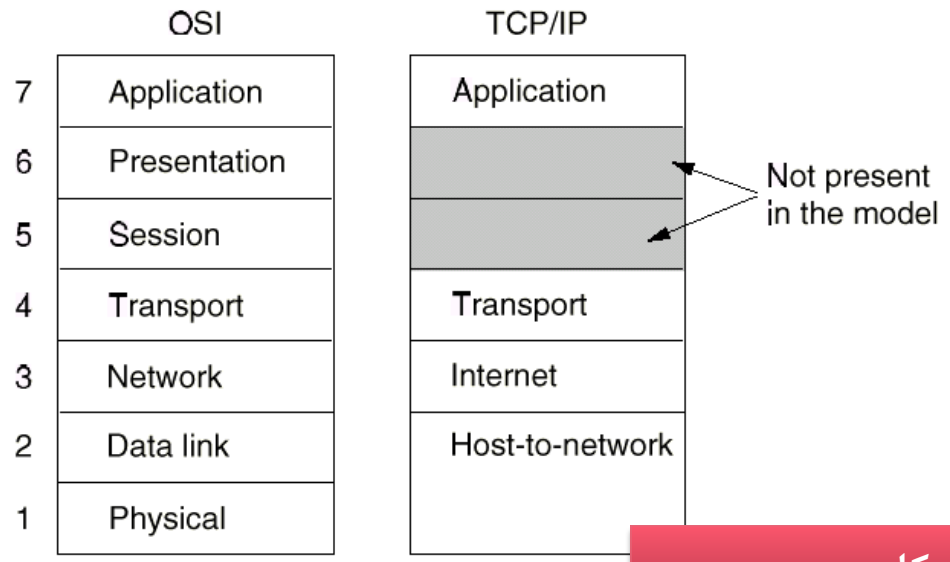
مدل TCP / IP

- مهم‌ترین لایه: لایه اینترنت (شبکه)
- IP (internet protocol)
  - بدون اتصال
  - مسیریابی بسته‌ها
- لایه انتقال TCP / IP
  - ارسال انتها-به-انتها
  - TCP: transmission control protocol
  - UDP : user datagram protocol

- لایه کاربرد
  - مخفی کردن پیچیدگی‌های لایه‌های پایین‌تر از دید کاربر و ارتباط با کاربر
  - TELNET: virtual terminal
  - FTP: file transfer protocol
  - SMTP: simple mail transfer protocol
  - DNS: domain name service
  - NNTP: network news transfer protocol
  - HTTP: hypertext transfer protocol
  - SNMP: simple network management protocol



مقایسه مدل‌ها



ملاحظات امنیت وب

- World Wide Web: برنامه کاربردی از نوع client/server بر روی اینترنت و TCP / IP

مشکلات:

- برخلاف سادگی استفاده از مرورگرها و ایجاد محتوای تحت وب، ساختار زیرین از پیچیدگی بالایی برخوردار است که موجب مخفی شدن آسیب‌پذیری‌های امنیتی می‌شود
- حمله به اطلاعات مخلی از طریق پایانه‌های متصل به شبکه
- وجود کاربرهای ناآشنا به امور امنیتی

تهدیدهای امنیتی 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

تهدیدهای امنیتی وب

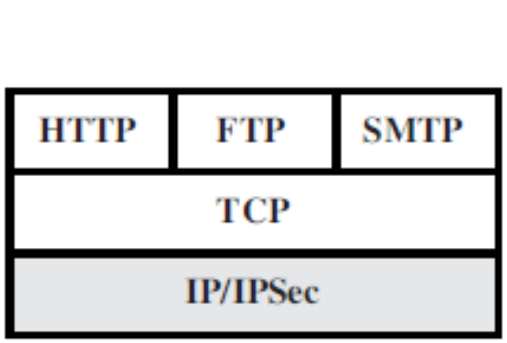
- تقسیم‌بندی بر اساس هدف مهاجم:
- حمله غیرفعال (Passive attack)
  - شنود (eavesdropping) ترافیک شبکه میان مرورگر و کارگزار و دسترسی به اطلاعات پایگاه وب که مخفی بوده
- حمله فعال (Active attack)
  - جعل هویت کاربر دیگر، تغییر پیام میان کارخواه و کارگزار، تغییر اطلاعات در یک پایگاه وب
- تقسیم‌بندی بر اساس مکان حمله:
- حمله به کارگزار وب
- حمله به مرورگر وب

امنیت سیستم

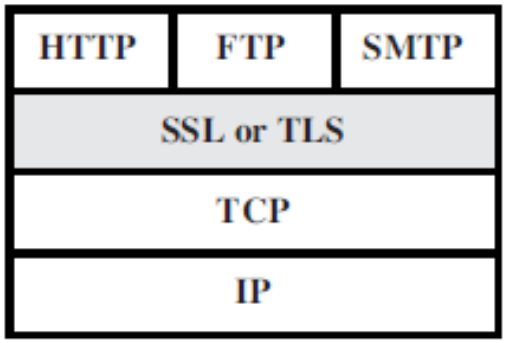
- حمله به ترافیک میان کارگزار و مرورگر (ترافیک شبکه وب)
  - امنیت شبکه

روش‌های تامین امنیت ترافیک وب

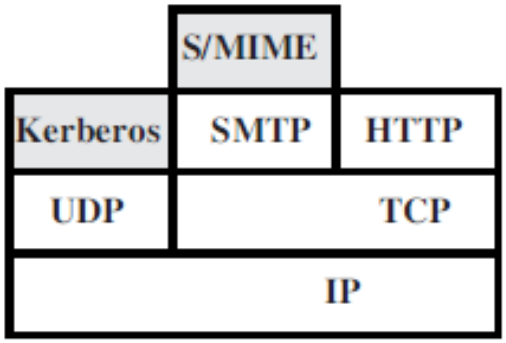
- خدمات یکسان و ساز و کارهای تقریباً مشابه
- تفاوت اصلی: مکان قرار داشتن در مدل TCP / IP و کاربرد آن‌ها
- سطح شبکه (استفاده از IPsec)
  - پنهان از دید کاربرهای انتهایی و برنامه‌های کاربردی
  - همه منظوره
  - خاصیت فیلترینگ به منظور کاهش سربار پردازشی IPsec



(a) Network level



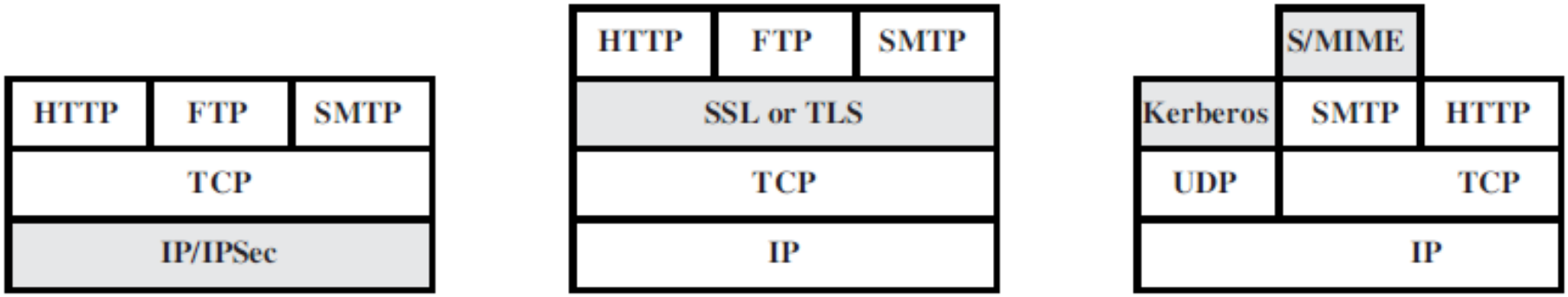
(b) Transport level



(c) Application level

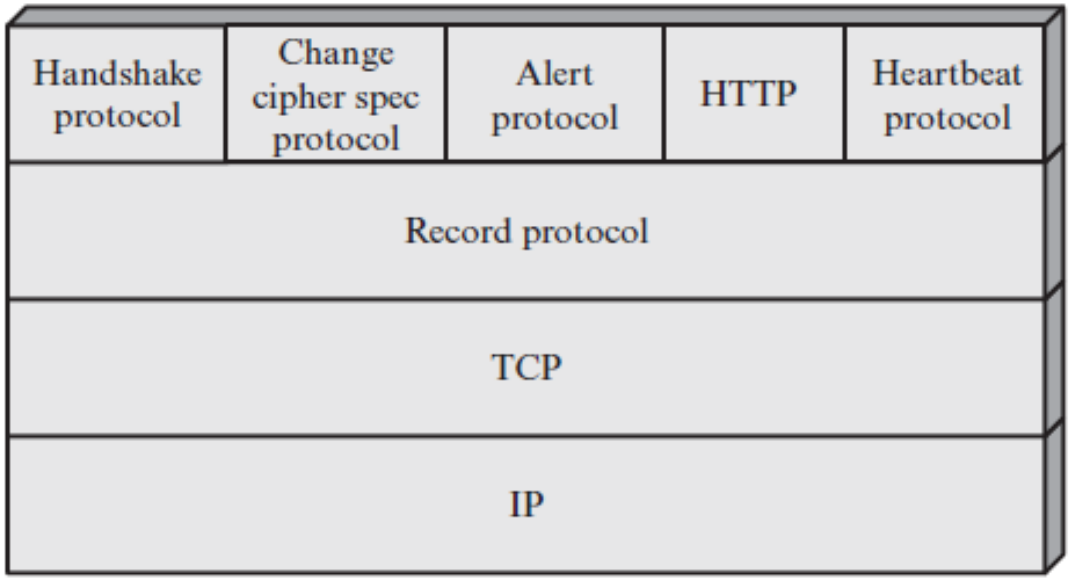
روش‌های تامین امنیت ترافیک وب

- سطح انتقال (بالای TCP)
  - Secure Sockets Layer (SSL) / استاندارد اینترنتی Transport Layer Security (TLS)
  - پشتیبانی بسیاری از سرورهای وب و تمامی مرورگرها
- سطح کاربرد
  - برآورد کردن تقاضای امنیتی خاص برای کاربردهای خاص



Transport Layer Security (TLS)

- نسخه کنونی ۱.۲
- استاندارد امنیتی برپایه پروتکل تجاری لایه دریچه امن Secure Sockets Layer (SSL)
- لایه امنیتی در بالای TCP جهت ایجاد خدمت امن انتها-به-انتها
- دو لایه پروتکلی
  - لایه اول در بالای TCP = پروتکل Record
    - محرمانگی و احراز اصالت پیام
  - لایه دوم در لایه کاربرد = ۳ پروتکل مدیریت مبادلات TLS
    - Handshake Protocol
    - Change Cipher Spec Protocol
    - Alert Protocol



مفهوم ارتباط در TLS

- اتصال (Connection)
  - یک انتقال (به مفهوم OSI) برای تامین خدمت مشخص
  - رابطه همتا-به-همتا (peer-to-peer)
  - هر اتصال به یک نشست نگاشت می‌شود (نگاشت چند به یک)
- نشست (Session)
  - هر نشست، یک ارتباط میان کلاینت و سرور است
  - هر نشست، توسط پروتکل دستداد (Handshake) شکل می‌گیرد
  - هر نشست، مجموعه‌ای از پارامترهای رمزنگاری را تعریف می‌کند که می‌تواند میان چندین اتصال مشترک باشد
    - جهت کاهش هزینه

حالت نشست (session state)

- نشست دارای (پارامترهای) حالت است که در پروتکل دستداد به روز می‌شوند
- پارامترهای حالت نشست:

Session identifier	An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
Peer certificate	An X509.v3 certificate of the peer. This element of the state may be null.
Compression method	The algorithm used to compress data prior to encryption.
Cipher spec	Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size.
Master secret	48-byte secret shared between the client and server.
Is resumable	A flag indicating whether the session can be used to initiate new connections.

حالت اتصال (connection state)

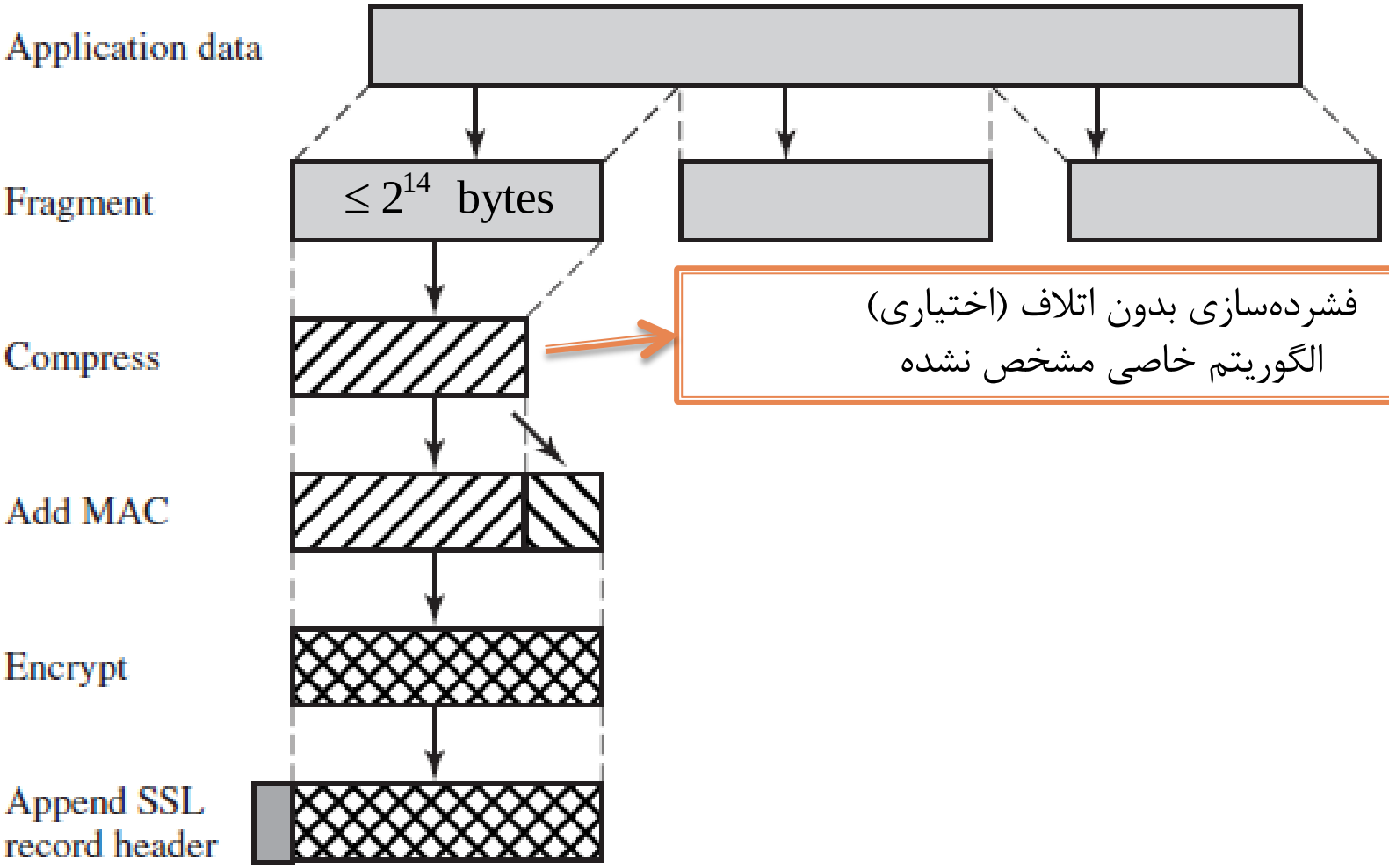
Server and client random	Byte sequences that are chosen by the server and client for each connection.
Server write MAC secret	The secret key used in MAC operations on data sent by the server.
Client write MAC secret	The secret key used in MAC operations on data sent by the client.
Server write key	The secret encryption key for data encrypted by the server and decrypted by the client.
Client write key	The symmetric encryption key for data encrypted by the client and decrypted by the server.
Initialization vectors	When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key.
Sequence numbers	Each party maintains separate sequence numbers for transmitted and received messages for each connection.

پروتکل TLS Record

دو خدمت را برای TLS تامین می‌کند:

- محرمانگی
  - با استفاده از یک کلید مخفی (رمزنگاری متقارن) که در پروتکل دستداد به اشتراک گذاشته شده است
- یکپارچگی پیام
  - با استفاده از کد احراز اصالت پیام (MAC) که کلید مخفی آن نیز در پروتکل دستداد به اشتراک گذاشته شده است
- شامل مراحل زیر:
  - تکه‌تکه کردن (fragmentation)، فشرده‌سازی، افزودن MAC، رمزگذاری و الصاق سرآیند (header)

پروتکل TLS Record



پروتکل TLS Record
افزودن MAC

- افزودن کد احراز اصالت پیام (MAC) با استفاده از یک کلید مخفی مشترک
  - الگوریتم HMAC با استفاده از تابع چکیده‌ساز MD5 یا SHA-1

$$\text{HMAC}_K(M) = \text{H}[(K^+ \oplus \text{opad}) \| \text{H}[(K^+ \oplus \text{ipad}) \| M]]$$

  - بر روی: شماره دنباله، نوع فشرده‌سازی، طول تکه و محتوای تکه فشرده شده

HMAC_hash(MAC_write_secret, seq_num || TLSCompressed.type ||
TLSCompressed.version || TLSCompressed.length || TLSCompressed.fragment)

پروتکل TLS Record
رمزگذاری

- پیام فشرده شده همراه با MAC، رمزگذاری می‌شود
  - در رمز قالبی، ممکن است نیاز به دنباله زدن (padding) باشد

Block Cipher		Stream Cipher	
Algorithm	**Key Size**	**Algorithm**	**Key Size**
AES 3DES	128, 256 168	RC4-128	128

پروتکل TLS Record
الصاق سر آیند (header)

- سرآیند=نوع محتوا، نسخه TLS، طول تکه فشرده شده (متن اصلی قبل از رمز)
- نوع محتوا (۸ بیت): پروتکل لایه بالاتر که تکه را پردازش می‌کند
  - change_cipher_spec, alert, handshake, application_data
    - کاربرد مانند HTTP
- نسخه اصلی و فرعی TLS مورد استفاده: برای TLSv2
  - اصلی=3، فرعی=1

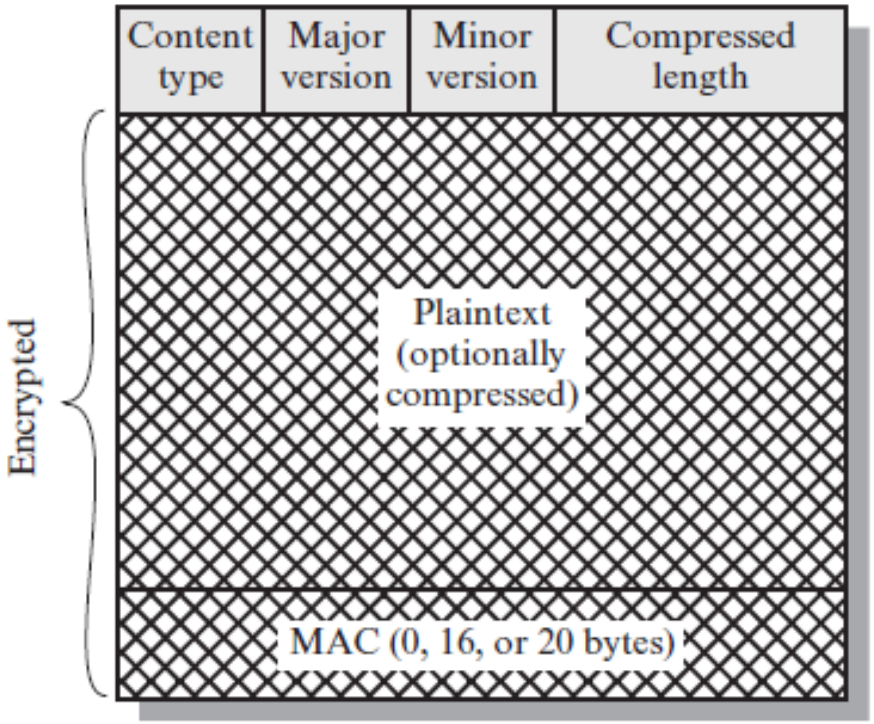
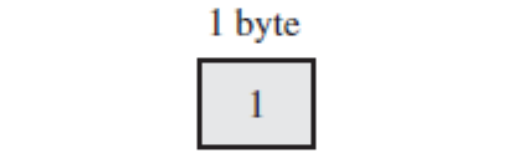


Figure 17.4 TLS Record Format

پروتکل Change Cipher Spec

- یکی از ۴ پروتکل لایه دوم که از پروتکل TLS Record استفاده می‌کنند
  - ساده‌ترین آن‌ها
- دارای یک پیام ۱ بایتی با مقدار ۱

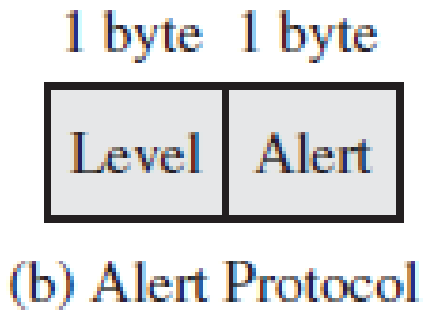
- در پایان پروتکل دستداد، منجر به جایگزینی CipherSpec در حالت نشست فعلی با یک حالت نشست جدید (حالت در انتظار (pending)) می‌شود
  - برای استفاده در اتصال جدید



(a) Change Cipher Spec Protocol

پروتکل هشدار (alert)

- هشدارهای (خطا) TLS را به همتا ارسال می‌کند
  - پیام‌ها فشرده شده و رمز شده = ۲ بایت
  - بایت اول= شدت (Level): warning (1) یا fatal (2)
  - پس از دریافت هشدار fatal، اتصال TLS خاتمه می‌یابد و اتصال جدیدی در نشست همراه آن برقرار نمی‌شود
  - بایت دوم (Alert): شامل کدی است که نوع هشدار را مشخص می‌کند



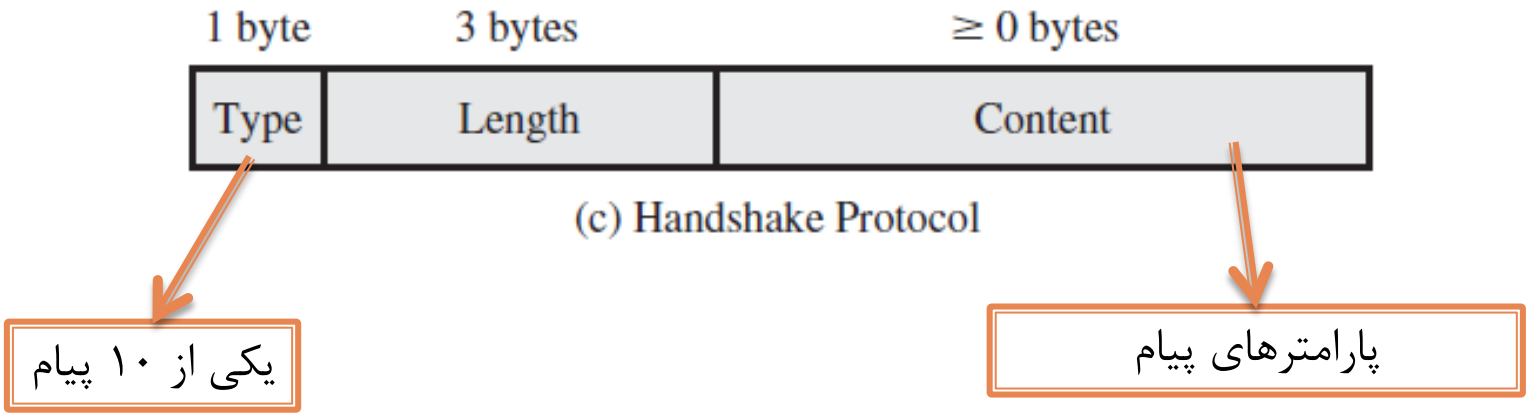
(b) Alert Protocol

برخی از هشدارها

unexpected_message	An inappropriate message was received.
bad_record_mac	An incorrect MAC was received.
decompression_failure	The decompression function received improper input.
handshake_failure	Sender was unable to negotiate an acceptable set of security parameters given the options available.
illegal_parameter	A field in a handshake message was out of range or inconsistent with other fields.
close_notify	Notifies the recipient that the sender will not send any more messages on this connection.
no_certificate	May be sent in response to a certificate request if no appropriate certificate is available.
bad_certificate	A received certificate was corrupt (e.g., contained a signature that did not verify).
unsupported_certificate	The type of the received certificate is not supported.
certificate_revoked	A certificate has been revoked by its signer.
certificate_expired	A certificate has expired.
certificate_unknown	Some other unspecified issue arose in processing the certificate, rendering it unacceptable.

پروتکل دستداد (Handshake)

- پیچیده‌ترین پروتکل TLS است که در آن کلاینت و سرور:
  - یکدیگر را احراز اصالت می‌کنند
  - بر روی الگوریتم رمزنگاری، الگوریتم MAC و کلیدهای مورد نیاز توافق می‌کنند
- پیش از هر ارسال داده (لایه کاربرد) صورت می‌گیرد
- تعدادی پیام میان کارخواه و کارگزار رد و بدل می‌شود
  - ۴ فاز



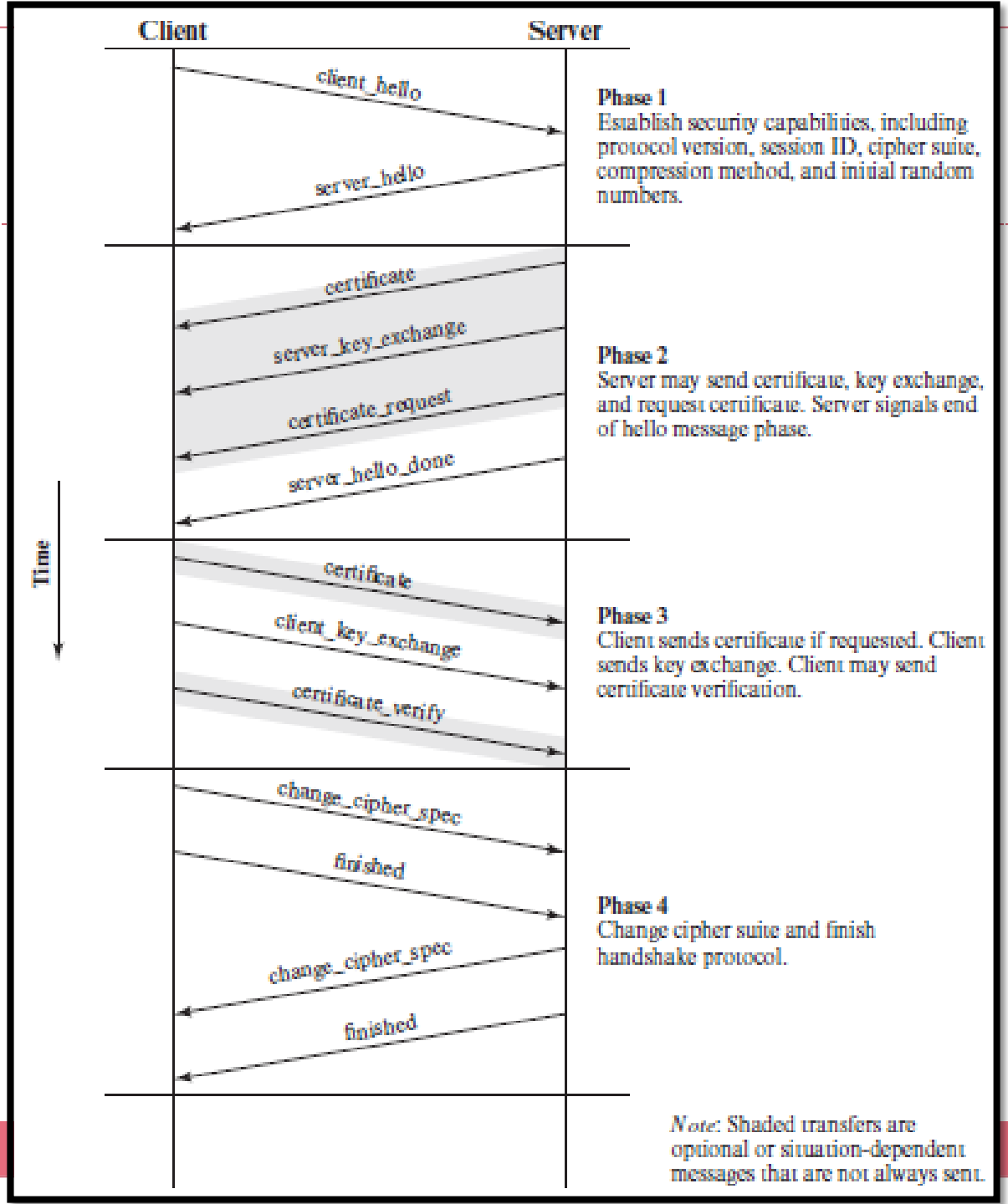
پیام‌های پروتکل دستداد

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

فازهای پروتکل دستداد

- شامل ۴ فاز

1. تعیین توانمندی‌های امنیتی کلاینت و سرور
2. احراز اصالت سرور به کلاینت و مبادله کلیدهای آن
3. احراز اصالت کلاینت به سرور و مبادله کلیدهای آن
4. پایان: تکمیل ایجاد اتصال امن با جایگذاری حالت


Client
Server
client_hello
server_hello
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

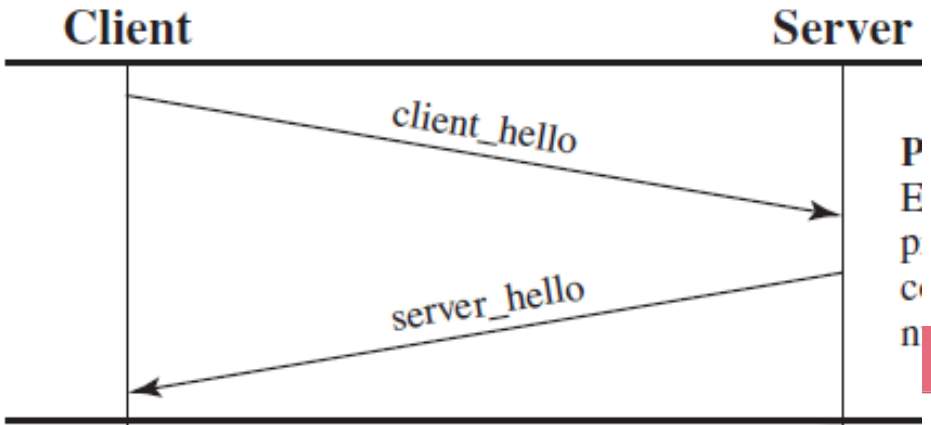
پروتکل دستداد: فاز ۱
تعیین توانمندی‌های امنیتی کلاینت و سرور

- ارسال توسط کلاینت:

client_hello=version, random, session id, cipher suite, compression method

فهرست الگوریتم‌های فشرده‌سازی پشتیبانی شده توسط کلاینت	فهرست الگوریتم‌های رمزنگاری پشتیبانی شده توسط کلاینت همراه با روش توافق کلید آن‌ها	0: نشست جدید i: به روز کردن پارامترهای نشست iام	عدد تصادفی استفاده برای تک‌شمار در توافق کلید جلوگیری از حمله تکرار	آخرین نسخه پشتیبانی شده توسط کلاینت

- پاسخ سرور با پیامی مشابه ولی با انتخاب الگوریتم‌های مناسب از فهرست‌ها



cipher suite

توافق کلید

RSA	The secret key is encrypted with the receiver's RSA public key. A public key certificate for the receiver's key must be made available.
Fixed Diffie-Hellman	Diffie-Hellman key exchange in which the server's certificate contains the Diffie-Hellman public parameters signed by the certificate authority (CA)
Ephemeral Diffie-Hellman	To create ephemeral (temporary, one-time) secret keys
Anonymous Diffie-Hellman	Diffie-Hellman algorithm is used with no authentication

CipherSpec

CipherAlgorithm	RC4, RC2, DES, 3DES, DES40, IDEA
MACAlgorithm	MD5 or SHA-1
CipherType	Stream or Block
IsExportable	True or False
HashSize	0, 16 (for MD5), or 20 (for SHA-1) bytes
Key Material	A sequence of bytes used in generating the write keys
IV Size	Size of the Initialization Value for Cipher Block Chaining (CBC) encryption

پروتکل دستداد: فاز ۲
احراز اصالت سرور به کلاینت و مبادله کلیدهای آن

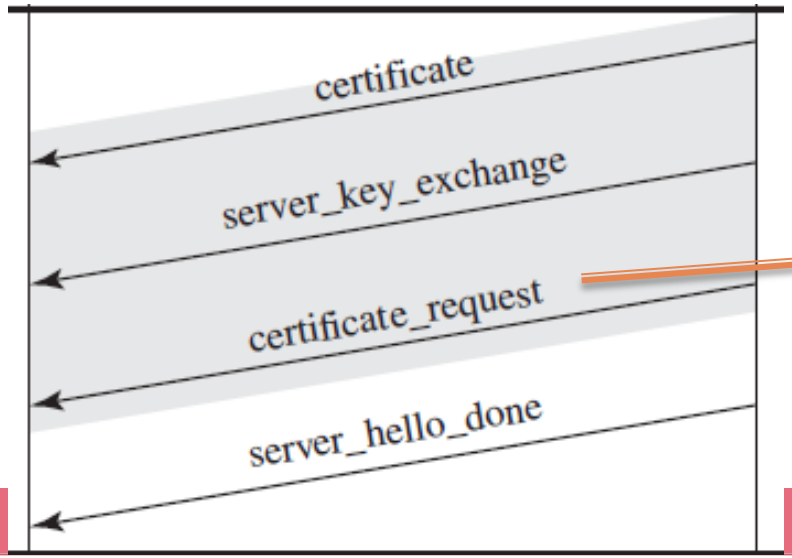
- ارسال گواهی سرور به کلاینت

Certificate = chain of X.509v3 certificates

server_key_exchange = parameters, signature ⟵ همیشه لازم نیست

امضا با استفاده از چکیده:

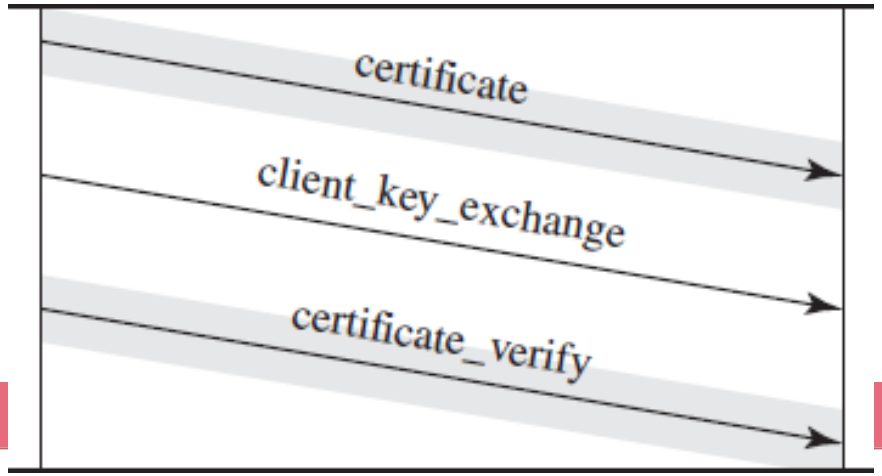
hash(ClientHello.random ‖ ServerHello.random ‖ ServerParams)



RSA, signature only
DSS, signature only
RSA for fixed Diffie-Hellman
(only for authentication)
DSS for fixed Diffie-Hellman
(only for authentication)

پروتکل دستداد: فاز ۳
احراز اصالت کلاینت به سرور و مبادله کلیدهای آن

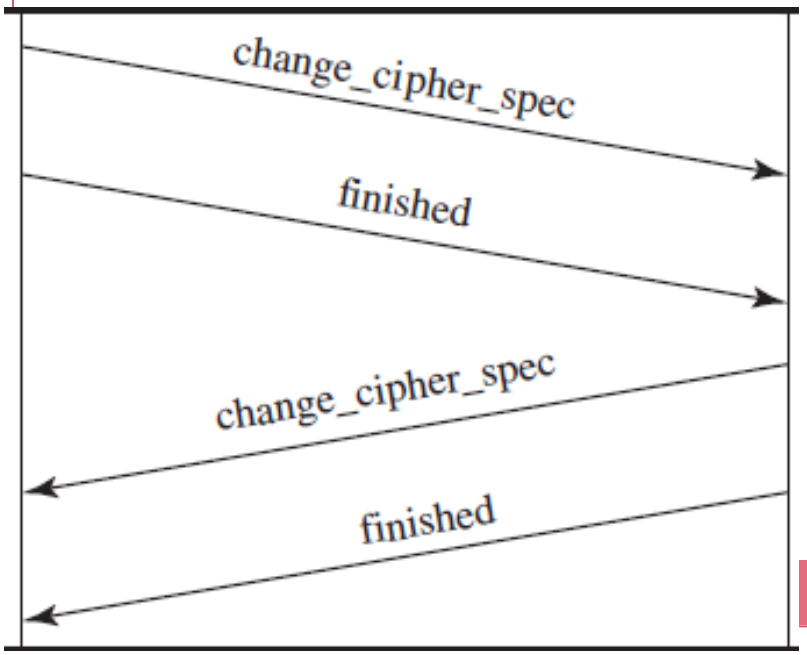
- کلاینت گواهی سرور را بررسی می‌کند و در صورت تایید پیام‌های این فاز را می‌فرستد
- در صورت درخواست گواهی از طرف سرور، ابتدا کلاینت گواهی خود را می‌فرستد
- پیام مبادله کلید وابسته به الگوریتم انتخاب شده است:
  - RSA: کلید مخفی را تولید و با کلید همگانی سرور (گواهی) رمز کرده و می‌فرستد
  - دیفی-هلمن: پارامترهای همگانی کلاینت ارسال می‌شود
- کلاینت چکیده تمامی پیام‌های قبلی را امضا کرده و می‌فرستد
  - تا سرور مطمئن شود که گواهی متعلق به کلاینت است



پروتکل دستداد: فاز ۴
پایان: تکمیل ایجاد اتصال امن با جایگذاری حالت

- کلاینت پیام change_cipher_spec را می‌فرستد و مقدار CipherSpec را در حالت به روز می‌کند
  - در اصل پیامی از پروتکل Change Cipher Spec
- پیام پایان (finished) با الگوریتم‌ها و کلیدهای جدید ارسال می‌شود

PRF(master_secret, finished_label, MD5(handshake_messages) || SHA-1 (handshake_messages))



  - چکیده تمام پیام‌های قبلی رمز و ارسال می‌شود
  - تایید موفقیت مبادله کلید و احراز اصالت

HTTPS

- ترکیب HTTP و SSL (و یا TLS) است
  - RFC 2818, *HTTP Over TLS*
- پیاده‌سازی ارتباط امن میان مرورگر وب و سرور وب
- پیاده‌سازی شده در تمامی مرورگرهای مدرن
  - استفاده از آن بستگی به کارگزار وب دارد
  - به عنوان مثال، برخی از موتورهای جستجو از HTTPS پشتیبانی نمی‌کنند
- HTTP: پورت 80
- HTTPS: پورت 443 که SSL را فرا می‌خواند
- موارد زیر **رمز** می‌شود:

URL of the requested document
Contents of the document
Contents of browser forms (filled in by browser user)
Cookies sent from browser to server and from server to browser
Contents of HTTP header

Secure Shell (SSH)

- Remote login and X tunneling