مدلOSI

(Open Systems Interconnection)

یک مدل مرجع برای ارتباط بین دو کامپیوتر می باشد.

کاربرد ---------->در اینترنت و معماری پایه شبکه (نشان‌دهنده‌ی یکی از معماری‌های مورد استفاده در شبکه‌های کامپیوتری است.)

هدف ----------> ارائه استانداردی به تولید کنندگان محصولات شبکه ای به منظور تولید محصولاتی سازگار با سایر تولید کنندگان است (جهت امکان کار با یکدیگر) .

این مدل بر اساس لایه بندی قراردادهای برقراری ارتباط که همزمان روی دو سیستم مرتبط اجرا شده اند پایه ریزی شده است که این امر بسیار سرعت و دقت ارتباط را افزایش می دهد(قبل از این مدل، استانداردی برای ارسال و دریافت پیام‌ها در شبکه وجود نداشت و مدل OSI برای رفع این نیاز تعریف شده است.)

از ۷ لایه‌ی مختلف ساخته شده است.

لایه‌های اول، لایه‌هایی مربوط به تبادل فیزیکی بسته‌ها هستند و لایه‌های بالاتر، بسته‌ها را به شیوه‌ی نرم‌افزاری انتقال می‌دهند. اساس کار این معماری به این شکل است که هر لایه، بدون آن‌که از جزییات کار لایه‌ی پایین‌تر خود آگاه باشد، از نتیجه‌ی عملکرد آن استفاده می‌کند و به لایه‌ی بالاتر خود سرویس می‌دهد.هر لایه، پروتکل‌های مخصوص به خود را دارد که اطلاعات را طبق استانداردهای آن پروتکل، درون بسته‌هایی قرار می‌دهد و هدرهایی را برای هر بسته مشخص می‌کند که اطلاعات لازم برای رسیدن بسته به مقصد را در خود دارند. هر یک از این بسته‌ها وقتی به مقصد می‌رسند، در همان لایه‌هایی که ایجاد شده‌اند، باز می‌شوند و محتویات آن‌ها به لایه‌ی بعدی تحویل داده می‌شود.

لایه‌های مدل OSI

جایی که اطلاعات به ۰ و ۱ تبدیل می شوند و رهسپار کابل میشوند...

۱ -لایه فیزیکی :(physical layer) ------> انتقال بیت‌های داده

۲ -لایه‌ی پیوند داده :(data link layer) ------> رساندن پیام‌های لایه‌ی فیزیکی به دست گیرنده است. رساندن پیام‌ها به دست گیرنده، با mac address انجام می‌شود)

_ بسته‌های این لایه frame نام دارند و از رایج‌ترین پروتکل‌های این لایه، می‌توان پروتکل PPP را نام برد.

۳ -لایه‌ی شبکه :(network layer)مسیریابی در شبکه به کمک پروتکل معروف این لایه یعنی IP انجام می‌شود. بسته‌های این لایه، packetنام دارند و هدرهای اینpacket ها، آدرس‌های IP مبدا و مقصد را مشخص می‌کنند.

۴ -لایه‌ی انتقال :(transport layer)------> ایجاد ارتباطی end-to-end بین مبدا و مقصد وکنترل جریان و کنترل خطا.

بسته‌های این لایه datagram نام دارند و پروتکل‌های اصلی این لایه، TCPو UDP هستند.

۵ -لایه‌ی نشست :(session layer)------> حفظ ارتباط بین ارسال‌کننده و دریافت‌کننده

۶ -لایه‌ی نمایش :(presentation layer) این لایه، اطلاعات دریافت شده از لایه‌ی بالایی خود را به زبانی قابل فهم برای لایه‌ی پایین‌تر خود ترجمه می‌کند

7- Application layer یا لایه کاربردی: بیش‌تر پیام‌هایی که در شبکه‌ی اینترنت مبادله می‌شوند، در این لایه تولید می‌شوند. این لایه رابط بین کاربر و سیستم عامل محسوب می شود

این لایه تنها لایه ای است که کاربر می تواند آن را بصورت ملموس حس کند و با آن ارتباط برقرار کند.(بوسیله این لایه با نرم افزارهای کاربردی ارتباط برقرار می کنید.)

پروتکل‌های آشنایی مانند HTTP و FTP (file transfer protocol) متعلق به این لایه هستند.(HTTP ، FTP، TELNET، SNMP، POP3)

مدلTCP/IP

(Transmission Control Protocol / Internet Protocol)

(پروتکل کنترل انتقال / پروتکل اینترنت)مهمترین پروتکل ارتباطی در شبکه های کامپیوتری و به ویژه شبکه اینترنت است.

پروتکل اولیه ارتباط به اینترنت است بدون TCP/IP عملاً اینترنتی هم وجود ندارد

لایه‌های مدل TCP/IP عبارت‌اند از :

۱ -لایه‌ی واسط شبکه :(network interface layer) آدرس‌هایMAC ، مسیریابی مربوط به آن‌ها و ارسال و دریافت فیزیکی بیت‌ها، مربوط به این لایه هستند.

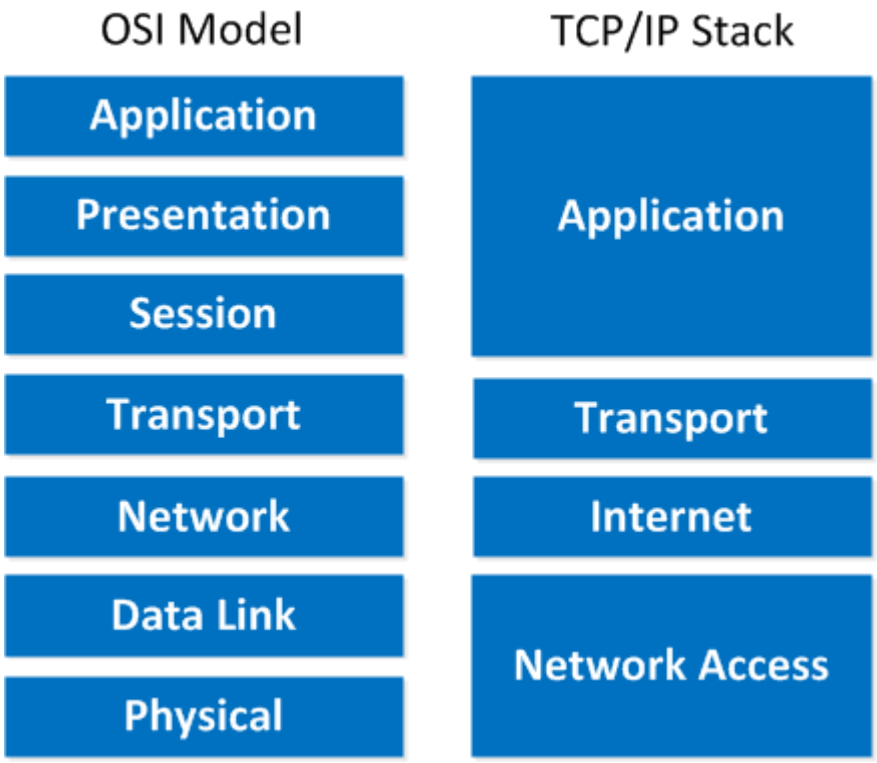
۲ -لایه‌ی اینترنت :(internet layer) مهم‌ترین پروتکل در این لایه، پروتکل اینترنت (internet protocol) یا IP است.

۳ -لایه‌ی انتقال :(transport layer) برقراری ارتباط بین دو host با استفاده از لایه‌های زیرین خود است تا از این راه بتواند اطلاعات لایه‌ی بالاتر خود را تا حد امکان بدون خطا به مقصد برساند.

پروتکل‌های اصلی این لایه، پروتکل‌های TCP و UDP هستند.

۴ -لایه‌ی کاربرد :(application layer)این لایه، ترکیب لایه‌هایapplication ، sessionو presentation در مدل OSI است. با کمک این لایه کاربر با کامپیوتر تعامل دارد و می‌تواند از آن برای ارسال و دریافت داده استفاده کند. هر بسته‌ی ایجاد شده در این لایه برای ارسال به لایه‌ی transport داده می‌شود تا به دست مقصد برسد. تمام پروتکل‌هایی که مربوط به سه لایه‌ی آخر مدل OSI هستند، مانندHTTP ، SSH، FTPو ...، در این دسته قرار می‌گیرند.

لایه های این دو مرجع:



تفاوت ها:

از نظر لایه‌ای بودن:

1- مدلTCP/IP ، لایه‌های کم‌تری نسبت به مدل OSI دارد. دلیل این تفاوت هم آن است که در معماری TCP/IP لایه‌هایی از OSI که عملکرد بسیار مشابه یا نزدیک داشته‌اند، در قالب یک لایه در نظر گرفته شده‌اند.
2- زمانی که مدل OSI طراحی شد، عملکرد پروتکل‌ها در نظر گرفته نشده بود و پس از طراحی و براساس نیاز، پروتکل‌ها ایجاد می‌شدند. اما طراحی مدل TCP/IP بر پایه‌ی پروتکل‌ها انجام شده است و لایه‌ها با توجه به عملکرد پروتکل‌ها تنظیم شده‌اند.

3- مدلOSI ، عموما به عنوان یک مدل مفهومی و برای درک بهتر شبکه‌ی طراحی شده، مورد استفاده قرار می‌گیرد. در حالی که مدلTCP/IP ، بیش‌تر کاربردی و عملن برای رفع برخی مشکلات شبکه و براساس رایج‌ترین پروتکل‌های آن طراحی شده است.

4- مدل مرجع TCP/IP ، بصورت کاربردی بیشتر از OSI مورد استفاده قرار می گیرد اما بعنوان مدل درسی و مدل تئوری برای یادگیری مورد استفاده قرار نمی گیرد

ping (Packet Internet or Inter-Network Groper)

ـ ابزاری برای تشخیص سالم بودن مسیر و گره یا سرور مقصد و همچنین مشخص کننده مقدار تاخیر برحسب میلی‌ثانیه (MS)است. می‌توان دریافت که چقدر طول خواهد کشید که یک بسته اطلاعات از سمت دستگاه هوشمند مانند کامپیوتر به سمت سرور رفته و دوباره از آن مسیر برگردد. پینگ درواقع تأخیر زمانی است که در هنگام انجام هر کار Online اتفاق میافتد، از کلیک بر روی لینک، تا استریم کردن یک ویدئو.

ـ یکی از ابزارها و برنامه‌های مورد استفاده در شبکه برای آزمایش در دسترس بودن یک آدرس آی پی یا دامنه (تست اتصال و اندازه گیری زمان)

- با استفاده از این ابزار می‌توان تاحدودی مشکلات شبکه را اشکال یابی کرد و ارتباطات TCP/IP را مورد ارزیابی قرار داد.

- دستوری جهت تعیین ارتباط، میزان سرعت و زمان برگشت بسته‌ها بین دو نقطه مختلف مثل دو کامپیوتر یا کامپیوتر با یک سایت می‌باشد. این فرمان معمولاً برای بررسی خطاهای شبکه استفاده می‌شود.(هر شبکه از تعداد متعددی دستگاه و سرور تشکیل‌شده است. پینگ دستوری است که این امکان را فراهم می‌کند مدت زمان رفت و برگشت Packet را بین دستگاه‌ها، اندازه بگیرید. استفاده از دستور پینگ برای چک کردن وضعیت سرورها بسیار مفید است.)

هرچقدر سرعت دریافت و ارسال اطلاعات بیشتر انجام گردد، عدد پینگ ما کوچکتر خواهد بود .(هرچقدر پینگ کمتر باشد سرویس اینترنت شما از کیفیت بهتری برخوردار است.)این عدد نشانگر کیفیت سرعت اینترنت ما یا سروری که به آن پینگ می‌گیریم، می‌باشد. پس از مشخص شدن این عدد می‌توانید از نتایج برای نتیجه گیری بیشتر استفاده کنید.به همین دلیل هنگام خطای اتصال به اینترنت، پینگ معمولاً اولین خط دفاعی شما محسوب می‌شود.

در کل پینگ با دو هدف انجام می‌شود:

------- > یکی اینکه بررسی کند آیا هاست در دسترس است یعنی به شبکه وصل است و در شبکه دیده می‌شود یا نه

------- > دوم اینکه مدت زمان دریافت پاسخ را اندازه بگیرد یعنی سرعت ارسال و دریافت اطلاعات چقدر است.

دستور پینگ چگونه کار می‌کند؟

پینگ با ارسال یک سیگنال درخواست، برای کامپیوتر دیگری، منتظر دریافت پاسخ می‌ماند. کامپیوتر دیگر پس از دریافت سیگنال از طریق پاسخ به آن سیگنال پاسخ می‌دهد. پروتکلی که برای درخواست و پاسخ دادن استفاده می‌شود، ICMP)پروتکل (Internet Control Message Protocol نام دارد. یک پروتکل سبک و روان که برای انتقال پیام‌های خطا و اطلاعاتی درباره شبکه استفاده می‌شود. ابزار پینگ زمان رفت و برگشت بسته و هرگونه تلفات در طول مسیر را اندازه گیری و ثبت می‌کند.

خروجی‌های دستور پینگ

فرمان ping دارای پارامترها و گزینه‌های مختلفی است که به شرح زیر هستند:

ping [-a] [-t] [-n] [-?] [IP address] [host name] [/?]

```
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprec
ated
                   and has no effect on the type of service field in the IP

                   Header).
```

خروجی دستور ping بستگی به نوع سیستم عامل دارد. اما تقریبا تمام خروجی‌های تست پینگ شامل موارد زیر است:

- Destination IP(آدرس مقصد IP)

- ICMP Sequence Number
- (Time to live) TTL
- Round-trip time
- Payload size

- Packet lost(تعداد بسته های گم شده در پروسه ارسال و دریافت)

برای استفاده از این قابلیت:

Cmd……ping <website> or ping <IP>….Enter

در خط اول دستور:

آدرس وبسایت مقصد شماره IP مقصد حجم بسته‌ی ارسالی

هر پاسخ شامل:

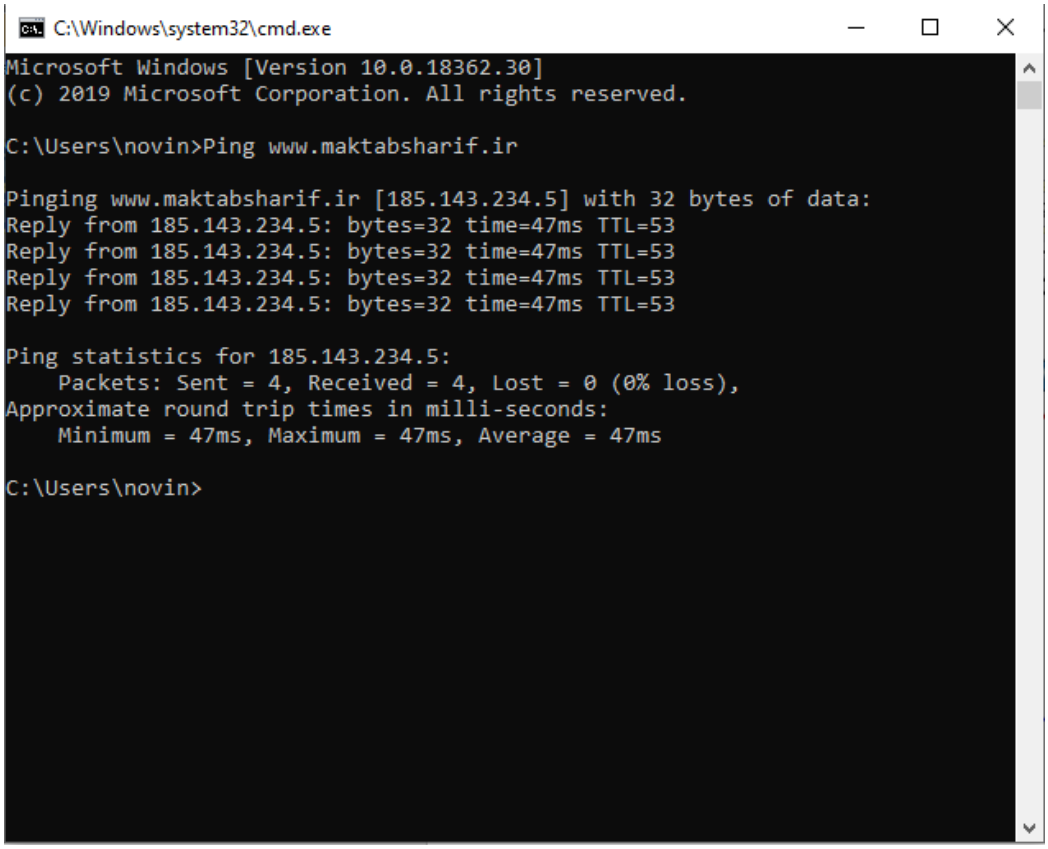
چهار خط بعدی، نمایانگر پاسخ دریافتی از هر بسته هستند که شامل موارد زیر می‌شوند:

اندازه بسته (بایت)

مدت زمان میلی‌ثانیه(:timeزمان پاسخ‌دهی که به میلی ثانیه نوشته شده است.)

TTL: طول عمر بسته (Time-To-Live) که نمایانگر زمانی است که اگر در طول آن پاسخی دریافت نشود، بسته دور ریخته خواهد شد.

تست پینگ سایت مکتب شریف



در انتهای دستور، یک خلاصه از وضعیت و تعداد بسته‌های ارسالی و دریافتی، به همراه حداقل، حداکثر و میانگین زمان پاسخ را مشاهده می‌کنید.

jitterچیست؟ Jitterدر شبکه چیست؟

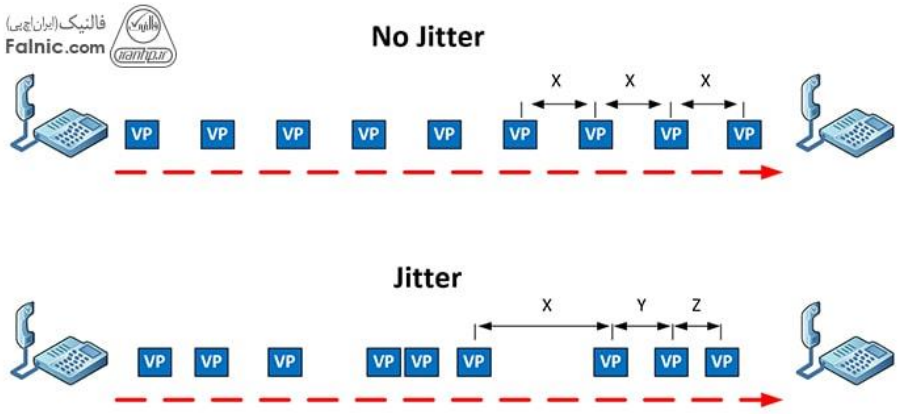
هر آنچه در اینترنت وجود دارد به شکل packet است: تمام تصاویر، متن ها، صدا و ویدئو در قالب بسته روی شبکه جابجا می‌شوند. در واقع. شما وقتی می خواهید اطلاعاتی را از نقطه A به سمت نقطه B ارسال کنید این اطلاعات در قالب بسته های اطلاعاتی از نقطه A به B در فواصل زمانی معین ارسال می شوند.ممکن است یک بسته اطلاعاتی در 20 میلی ثانیه و یک بسته اطلاعاتی در 10 میلی ثانیه و بعدی در 60 میلی ثانیه از A به B برسد یعنی تنوع زمانی انتقال اطلاعات در شبکه ، این همان Jitter است ، به Jitter در برخی اوقات Packet Delay Variation هم گفته می شود که به معنی تنوع اندازه تاخیرها در بسته های اطلاعاتی می باشد.

.به طور کلی در جواب سوال jitterچیست، می توان گفت، زمانی که در تاخیر بسته ها، تفاوت ایجاد شد، jitterرخ می دهد.

در اکثر شبکه ها جیتر وجود دارد .و به طور ایده آل بهتر است این تاخیر ها زیر ۳۰ میلی ثانیه باشد .

راهکارهای برطرف کردن Jitter در شبکه

عیب یابی جیتر شبکه بسیار مشکل است زیرا جیتر به طور پیش‌بینی نشده رخ می‌دهد. اگر شبکه را به درستی پیاده‌سازی کرده باشید، جیتر در حداقل خواهد بود. کیفیت اتصالات شبکه، پهنای باند کافی و تاخیر قابل پیش‌بینی باعث کاهش جیتر در شبکه می‌شود .آپگرید کردن کابل اترنت ،بررسی فرکانس کاری تجهیزات،کاهش مصرف پهنای باند با قطع دستگاه های متصل خصوصا در ساعات کاری،گرفتن تست پهنای باند



پروتکل telnet :

23……..> udp

24……> tcp

پروتکل Telnet یا Terminal Network یک پروتکل ارتباطی شبکه کامپیوتری است که در اینترنت و شبکه های محلی برای ارتباط دو طرفه دستوری از طریق CMD (Command Terminal) می باشد.

اگر بخواهید از راه دور به سرور خود متصل شوید و دستور خاصی را در آن اجرا کنید، راه های مختلفی برای اینکار وجود دارد که Telnet هم یکی از آنهاست .

پروتکل RDP:

Remote Desktop Protocol

server listens on TCP port ……..>3389 UDP port ……..>3389

یک پروتکل اختصاصی است که یک رابط گرافیکی را برای کاربر فراهم می کند تا از طریق اتصال شبکه به رایانه دیگر متصل شود. کاربر از نرم افزار مشتری RDP برای این منظور استفاده می کند ، در حالی که رایانه دیگر باید نرم افزار سرور RDP را اجرا کند.

پروتکل Imap:

Internet Message Access Protocol……..> 143

پروتکل IMAP مخفف Internet Message Access Protocol می باشد که به معنی پروتکل دستیابی به پیغام در اینترنت است.
imap یکی از پروتکل های مورد استفاده در اینترنت است. از این پروتکل برای انتقال و ارتباطات ایمیل در وب بهره می گیرند

بطور مثال سرویس های صندوق پست الکترونیکی و یا وب سایت های جدید که امروزه فایلهای صوتی و تصویری در آن ها بصورت آنلاین Online مورد استفاده قرار می گیرند از این پروتکل بهره گرفته اند. پروتکل IMAP در لایه کاربردی و بر روی پورت شماره ی ۱۴۳ قرار دارد وبه سرویس گیرنده ها اجازه دسترسی به ایمیل بر روی سرویس دهنده از طریق کنترل از راه دور را فراهم می کند..

پروتکل icmp :

Protocol Number 1

پروتکل icmp یک بخش جدانشدنی از پروتکل ip است و از اساسی ترین و پایه ترین پروتکل های کاربردی میباشد

پروتکل icmp که مخفف عبارت internet control message protocol است که در فارسی آن را پروتکل کنترل پیام های اینترنتی ترجمه می کنند. icmp جهت خطایابی در کامپیوترها ، روترها و هاست، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرور ها مورد استفاده قرار می گیرد.

رمزنگاری نامتقارن

Asymmetric cryptography

اینترنت پراز درخواست ها وجواب های است که به درخواست پاسخ می دهند....در این بین برای secureکردن روابط اول از رمز نگاری متقارن استفاده شد که امنیت نسبتا پایینی داشت ،. که نیاز به رمزنگاری نامتقارن را ایجاد کرد

برای هر شخصی هر دو کلید ساخته میشود(کلید عمومی :Public Key و کلید خصوصی:Private Key) و اطلاعات کاید عمومی فقط با کلید خصوصی باز می شود ... پس اگر من اطلاعاتم رو با کلید عمومی از طریق نت یا هر چیز دیگری برای طرف مقابلم ارسال کنم و جواب دریافت کنم ..دراین بین هیچ کس نمیتواند این اطلاعات را رمزنگاری کند ..چون فقط با کلید خصوصی که من در دسترس دارم قابل رمزنگاری هست .

قسمت جالب اینه که میتونه من رو شناسایی یا Authenticateکنه که هر کسی میتونه امضای شخصی داشته باشه ....به اینصورت که یه متنی رو باکلید خصوصی مینویسه پس هرکس که با کلید عمومی این اطلاعات من رو باز کنه امضای من رو میبینه

SSL یا TLS

مخفف عبارت Secure Sockets Layer به معنی «لایه سوکت های امن» است.

SSLیک فناوری امنیتی استاندارد برای برقراری یک پیوند رمزگذاری شده بین یک سرور و یک مرورگر است. این پیوند امن، محرمانه باقی ماندن تمامی داده‌هایی که بین سرور و مرورگر رد و بدل می‌شوند را تضمین می‌کند.

اگر وبسایتی با SSL رمزگذاری شده، مرورگر شما گواهینامه SSL را بررسی می‌کند و یک ارتباط واقعاً امن را بین مرورگر و سرور برقرار می‌کند. در این حالت هیچ‌کس به‌جز شما و وب‌سایتی که اطلاعاتتان را برای آن ارسال می‌کنید نمی‌تواند به آنچه که در مرورگر خود تایپ می‌کنید دسترسی داشته باشد یا آن اطلاعات را به هر نحوی مشاهده کند.

من gmail.comدرخواست میدم که این پروتوکل با این شکل رمزنگاری برای من ارسال کن..که کلید publicرو برام میفرسته....من بهش جواب میدم (increaption key) که یک پسورد هست .... و موافقت از طرف جی میل دریافت میکنم....

حالا از کجا مطمین بشم طرف من جی میل هست؟ این وسط اشخاصی هستن که کی های خصوصی میسازن (CA) ادرس کلید رو به CAمیفرستم و میپرسم که این طرف من هست ؟ در صورت تایید مطمئن میشم ....

هنگامی‌که وارد صفحه‌ای می‌شوید که حاوی یک فرم است، بعد از آنکه فرم مزبور را تکمیل کردید و دکمه ارسال را فشردید، اگر آن صفحه گواهی SSL نداشته باشد تمامی اطلاعاتی که در فرم مزبور وارد کرده‌اید توسط هکرها قابل مشاهده خواهد بود.این اطلاعات می‌تواند هر چیزی باشد؛ از اطلاعات تراکنش‌های بانکی گرفته تا اطلاعات خصوصی مهمی که برای ثبت نام در سرویس‌های مختلف وارد می‌کنید. هکرها به این سرقت اطلاعات، «حمله مرد میانی) «به انگلیسیman-in-the-middle attack)می‌گویند. حمله مزبور را از روش‌های مختلفی می‌توان انجام داد، اما یکی از رایج‌ترین روش‌های آن از این قرار است: هکر یک برنامه کم حجم و غیرقابل شناسایی جاسوسی را بر روی سروری که از وب‌سایت مورد نظر میزبانی می‌کند قرار می‌دهد. این برنامه در پس زمینه منتظر می‌ماند تا بازدیدکننده‌ای وارد یک وب‌سایت شود و درج اطلاعات در یکی از فرم‌های آن را آغاز کند؛ برنامه ذکرشده با درج اطلاعات فعال می‌شود، اطلاعات مربوطه را ثبت می‌کند و آن‌ها را برای هکر می‌فرستد؛

مزایایSSL

SSL .از اطلاعات محافظت می‌کند:کار اصلی گواهی SSL حفاظت از اطلاعاتی است که در ارتباط بین کاربر با سرور رد و بدل می‌شود. با نصب SSL هر بیت از داده‌ها رمزگذاری خواهد شد؛ به زبان ساده، اطلاعات قفل می‌شوند و کلید بازگشایی این قفل فقط در اختیار دریافت کننده مورد نظر قرار دارد.

SSLهویت شما را تأیید می‌کند

SSL .**باعث بهبود رتبه شما در نتایج موتورهای جستجو می‌شود**