درس:

کارگاه مدیریت و سنجش شبکه های گسترده

مدرس: اسماعیل طغرایی

ایمیل: Toghraee_University@yahoo.com
وب سایت ها: https://Teach.toghraee.ir
https://Toghraee.ir

دوره های تدریس:

- ✓ طراحی و پیاده سازی وب سایت HTML، PHP و...
- ✓ شبکه های کامپیوتری Network+
- ✓ دوره های CCNA و Intro
- ✓ برنامه نویسی C# و JS و Matlab
- ✓ طراحی و پیاده سازی وب سایت

چگونه کلمه عبور مناسب بسازیم و از آن نگهداری کنیم؟

رمز عبور یا همان پسورد شما، کلیدی است که برای دسترسی به اطلاعات شخصی خود که در کامپیوتر و حساب های آنلاین ذخیره کرده اید، به کار می رود. .....

چه عواملی یک پسورد را در مقابل حملات، قدرتمند می سازد؟

- یک پسورد قوی، باید به صورت رشته ای تصادفی از کاراکترها باشد. معیارهای زیر می تواند به این امر کمک کند:
- **طولانی بودن :**هر کاراکتری که شما به رمز عبور خود اضافه می کنید، حفاظت ایجاد شده به وسیله آن را چندین برابر افزایش می دهد. طول کلمه عبور شما باید 8 کاراکتر و یا بیشتر باشد. 14 کاراکتر یا بیشتر ایده آل است.
- **ترکیب حروف، اعداد و علائم :**هر چقدر تنوع کاراکترهایی که در رمز عبور استفاده می شود، بیش تر باشد، حدس زدن آن دشوارتر می گردد.
- سایر جزئیات مهم عبارتند از:
- هر چه تنوع کاراکترها کمتر باشد، پسورد باید طول بیشتری داشته باشد. اگر شما نمی توانید کلمه عبوری شامل علامت ها بسازید، نیاز دارید برای داشتن همان درجه از حفاظت، آن را به طور قابل ملاحظه ای طولانی تر کنید.
- از سرتاسر صفحه کلید (و نه فقط کاراکترهای رایج) استفاده کنید. سمبل هایی که با نگه داشتن دکمه "shift" و زدن یک عدد تایپ می شوند مانند @، #، % و ... در کلمات عبور بسیار مرسوم اند. در صورتی که از تمامی علامت های روی صفحه کلید از جمله علائم نقطه گذاری مانند ? ، ! ، " و ... استفاده شود، پسورد شما بسیار قوی تر خواهد شد.
- از کلمات و عبارت هایی که به یاد آوردن آن برای شما آسان است اما حدس زدن آن برای دیگران دشوار می باشد، استفاده کنید. ساده ترین راه برای به خاطر آوردن پسوردها و عبارات عبور، نوشتن آن ها بر روی کاغذ می باشد.
- بر خلاف باور عموم، نوشتن رمز عبور اصلا کار اشتباهی نیست، اما به منظور امن ماندن آن، باید به اندازه کافی محافظت شود. به طور کلی، رمز عبور نوشته شده بر روی یک تکه کاغذ، نسبت به رمز عبور ذخیره شده در وب سایت ها و دیگر ابزارهای نرم افزاری مانند نرم افزار مدیریت پسورد، در هنگام استفاده از اینترنت کم تر به خطر می افتد.

ساختن یک پسورد قوی که بتوان به یاد آورد

راه های زیادی برای ساختن یک کلمه عبور طولانی و پیچیده وجود دارد. در این جا روشی معرفی می کنیم که یادآوری آن را نیز ساده می سازد.

مثال	پیشنهاد	روش کار
Long and complex passwords are safest. I keep mine secret.	به چیزهایی که برای شما با معنی است فکر کنید.	با یک یا دو جمله در حدود 10 کلمه شروع کنید.
lacpasikms (10 characters)	از اولین حرف هر کلمه استفاده کنید.	جمله خود را به حروف پشت سر هم تبدیل کنید.
lACpAsIKMs (10 characters)	حروف نیمه اول الفبا را بزرگ کنید.	پیچیدگی را بیشتر کنید.
lACpAs56IKMs (12 characters)	یک عدد دو رقمی که برای شما معنی دارد را در بین دو جمله قرار دهید.	طول را با اعداد افزایش دهید.
?lACpAs56IKMs (13 characters)	یک کاراکتر نقطه گذاری در ابتدا اضافه کنید.	طول را با علائم نقطه گذاری زیاد کنید.
?lACpAs56IKMs@ (14 characters)	یک کاراکتر سمبل به انتها اضافه کنید.	طول را با سمبل ها افزایش دهید.

پسورد جدید خود را با Password Checker تست کنید .

Password Checkerابرازی است که قدرت پسورد شما را به طور اتوماتیک، در حین تایپ کردن ارزیابی می کند. برای استفاده از آن روی لینک زیر کلیک کنید .

https://www.microsoft.com/protect/fraud/passwords/checker.aspx

مدرس: اسماعیل طغرایی

الگوهای خطرناک پسورد که باید از آن اجتناب شود

مجرمان سایبری از ابزارهای پیچیده ای که می تواند به سرعت رمزهای عبور را کشف کند، استفاده می کنند. برخی از روش های معمول مورد استفاده برای ایجاد کلمات عبور، به سادگی توسط هکرها حدس زده می شود. برای اجتناب از ایجاد پسوردهای ضغیف که به آسانی حدس زده می شود، باید از موارد زیر دوری کنید:

- **جملات و کاراکترهای تکراری**"12345678" :، "222222"، "abcdegf"و یا حروف کنار هم در صفحه کلید شما، کمکی به ساخت یک پسورد امن نمی کند.
- **استفاده تنها از جایگزینی حروف با اعداد و سمبل های مشابه :**تبهکاران و یا دیگر افراد خرابکار که به حد کافی برای شکستن رمز عبور شما آگاه هستند، با این جایگزینی های رایج مانند عوض کردن "i" با "1" و یا "a" با "@" به عنوان مثال در کلمات "M1cr0$0ft" و"P@ssw0rd" ، فریب نمی خورند. اما زمانی که این جایگزینی های با معیارهای دیگر مانند طول پسورد، غلط املایی و دگرگونی ساختار کلمه عبور و جابجایی اجزای آن، ترکیب شود، می تواند برای بهبود استحکام رمز عبور شما موثر باشد.
- **استفاده از نام کاربری خود :** هر قسمت از نام، تاریخ تولد و شماره شناسنامه شما و یا اطلاعات مشابه در مورد عزیزانتان، انتخاب بدی برای ساخت پسورد می باشد. آن ها یکی از اولین مواردی است که مجرمان امتحان می کنند.
- **کلمات موجود در فرهنگ لغت هر زبانی** :مجرمان از ابزارهای پیچیده ای استفاده می کنند که می تواند به سرعت پسوردهایی که بر اساس واژه های موجود در چندین فرهنگ لغت (شامل کلماتی که برعکس خوانده می شود، غلط های املایی و جایگزینی های متداول) ساخته می شود را حدس بزنند.
- **استفاده از یک رمز عبور در همه جا :**اگر هر کدام از کامپیوترها و یا سیستم های آنلاین که از این پسورد مشترک استفاده می کند به خطر بیفتد، باید در نظر گرفته شود که تمام اطلاعات دیگر شما که توسط این رمز حفاظت می شود نیز به خطر خواهد افتاد. این نکته بسیار حیاتی و حائز اهمیت است که برای سیستم های مختلف از کلمات عبور متفاوت استفاده شود.
- **سیستم های ذخیره سازی آنلاین** :اگر افراد خرابکار به این پسوردهای ذخیره شده در سیستم های آنلاین و یا روی یک کامپیوتر در شبکه مانند سرور، دسترسی پیدا کنند، آن گاه به همه اطلاعات شما دسترسی پیدا می کنند.

5.نکته برای این که پسورد خود را مخفی نگاه دارید

1. **هرگز رمز عبور خود را در یک ایمیل و یا بر اساس یک درخواست ایمیلی وارد نکنید .**هر ایمیلی که پسورد شما را درخواست می کند و یا از شما می خواهد که با مراجعه به یک وب سایت، رمز عبور خود را برای تصدیق صحت وارد کنید، اغلب تقلبی و برای فریب شما است. این شامل درخواست از شخص و یا شرکت مورد اعتماد نیز می باشد. محتویات پست الکترونیکی در حین انتقال می تواند خوانده شود و ایمیلی که درخواست اطلاعات می کند، ممکن است از طرف فرستنده ای که آن را مطالبه کرده، نباشد. کلاهبرداری های اینترنتی فیشینگ از این ایمیل های جعلی به منظور فریب دادن شما برای افشای نام کاربری و پسورد، سرقت هویت و اطلاعات شما، استفاده می کنند.
2. **کلمه عبور را در کامپیوترهایی که بر روی آن ها کنترل ندارید تایپ نکنید .**کامپیوترهای اشتراکی مانند آن هایی که در کافی نت ها، دانشگاه ها، سالن های کنفرانس و سالن انتظار فرودگاه است، باید در نظر گرفته شود که برای استفاده های شخصی نا امن هستند. از این کامپیوتر ها برای چک کردن آنلاین پست الکترونیک، چت کردن، دیدن صورت حساب های بانکی، و یا هر حساب دیگری که نیاز به یک نام کاربری و رمز عبور دارد، استفاده نکنید. مجرمان از ابزارهای ثبت کردن دکمه های زده شده صفحه کلید استفاده می کنند. این ابزار به افراد خرابکار این امکان را می دهد که تمام اطلاعات تایپ شده بر روی یک کامپیوتر از جمله پسورد شما را از طریق اینترنت به دست آورند.
3. **آن ها را برای دیگران افشا نکنید .**رمز عبور خود را از دوستان و اعضا خانواده (خصوصا کودکان) که می توانند آن را به افراد دیگر منتقل کنند، مخفی نگاه دارید. پسوردهایی که نیاز دارید با دیگران به اشتراک بگذارید، مانند رمز عبور حساب بانکی آنلاین شما که ممکن است با همسر خود به اشتراک گذارید، تنها استثناها هستند.
4. **از پسورد خود محافظت کنید** .مراقب باشید که رمز عبور ذخیره شده و یا یادداشت شده خود را کجا نگه داری می کنید. پسوردها را بر روی یک فایل در کامپیوتر ذخیره نکنید، زیرا که مجرمان ابتدا آن جا را نگاه می کنند. کلمه عبور مورد استفاده خود را در یک مکان امن و مطمئن نگه داری کنید.
5. **رمز عبور خود را به طور منظم تغییر دهید .**با این کار مجرمان و دیگر افراد خرابکار را برای کشف پسورد خود به طور مداوم ناکام می گذارید. هر چه قدرت کلمه عبور شما بیشتر باشد، از آن می توان برای زمان طولانی تر استفاده کرد. پسوردی که کمتر از 8 کاراکتر باشد، باید در نظر گرفته شود که برای حدود یک هفته کارایی دارد، در حالی که پسوردی که 14 کاراکتر یا بیشتر باشد (و از قوانین دیگر ذکر شده در بالا تبعیت کند) می تواند برای چندین سال کارآمد باشد.

با زياد شدن دزد هاي شارژ اينترنت كم كم همه به فكر افتادن تا هر چند روز يك بار رمز واي فاي شان را تغيير بدهند تا ديگر كسي نتواند به شارژ اينترنت شان دسترسي داشته باشد.

شايد مسئله دزدي شارژ اينترنت فقط در ايران مطرح باشد چون در كشورهاي ديگر هزينه شارژ اينترنت انقدر ها زياد نيست كه كسي به فكر دزدي شارژ بيفتد! اما به هر حال تغيير رمز واي فاي در هر جاي دنيا يك مسئله كاملا ضروريست كه در ادامه اين مطلب دليل آن را خدمت شما توضيح ميدهيم.

- **دليل تغيير رمز مودم هاي واي فاي چيست ؟**
- هيچ كسي دوست ندارد كسي بدون اجازه وارد حريم خصوصيش بشود يا اينكه ديگران بدون اجازه از وسايل و لوازم شخصيش استفاده كنند. از اين رو تغيير رمز واي فاي بنا به دو دليل ضروريست:

- **1جلوگيري از دزدي اطلاعات شخصي –**
- متاسفانه خيلي ها اصلا متوجه اين مسئله نيستند كه هكر ها براي دزدي اطلاعات شخصي كاربران چه امكاناتي را در اختيار دارند! سيستم عامل هايي كه عموم مردم از آن استفاده ميكنند امنيت كافي براي محافظت از اطلاعات شخصي شما را ندارند و به راحتي نفوذ پذيرند.
- از طرفي كار كردن با سيستم عامل هاي امن مانند لينوكس براي همه ساده نيست و عموم مردم موقع كار كردن با لينوكس با مشكلات ريز و درشت زيادي مواجه ميشوند. شبكه هاي كامپيوتري بهترين راه براي هكر هاست تا به سيستم شما (چه لپ تاپ چه موبايل) نفوذ كنند و اطلاعات شخصيتان را بدزدند! تغيير مداوم رمز واي فاي دست بسياري از هكر ها رو قطع ميكند. فراموش نكنيد كه تغيير رمز واي فاي فقط يك راه حل ساده است و لازم است بدانيد كه با تغيير رمز واي فاي نميشود هكر هاي حرفه اي رو متوقف كرد!

- **2جلوگيري از دزدي شارژ اينترنت –**
- متاسفانه چون در ايران هزينه اينترنت بسيار بالاست، شارژ دزدي خيلي زياد شده است. اگرچه ريشه اين ناهنجاري فرهنگي صرفا هزينه هاي اينترنت نيست اما مسئله هزينه مي تواند انگيزه شارژ دزدي را در افراد به خصوص نوجوانان ايجاد كند.

توکن امنیتی

توکِن امنیتی یا **نشانهٔ امنیتی** (Security Token) سختافزاری کوچک است که برای ورود کاربر یک سرویس رایانه‌ای به سامانه بهکار میرود. به عبارت دیگر، این دستگاه یک دستگاه فیزیکی است که در اختیار کاربران مجاز قرار میگیرد تا به راحتی بتوانند برای استفاده از یک سیستم کامپیوتری هویت آنها تشخیص داده شود. توکن امنیتی برای اثبات هویت فرد به صورت الکترونیکی استفاده میشود.(به عنوان مثال نحوه دسترسی به حساب بانکی از راه دور). از توکن به علاوه یا به جای رمز عبور معمولی برای احراز هویت مشتری که خواهان ورود به سیستم است، بهره میبرند. به عبارت دیگر به عنوان یک کلید الکترونیکی برای دسترسی عمل میکند.

بعضی از توکنها کلیدهای رمزنگاری مانند امضا دیجیتال و اطلاعات بیومتریک مثل اثرانگشت را در حافظه خود ذخیره میکنند. [1] این توکنها شامل چند کلید برای وارد کردن پینکد یا شماره شناسایی شخصی) و آغاز برنامه توکن برای انجام عملیات ایجاد رمز عبور هستند. طراحی مخصوصی از این توکن به صورت ارتباطUSB و بلوتوث است که این روشها در انتقال کلید رمز تولید شده به سیستم دخالت دارند.

مجموعه‌ای از چند توکن امنیتی با روشهای گوناگون استفاده. در شکل یک سکه یک سنتی برای مقایسه اندازه قرار دارد.

انواع نشانه و موارد استفاده

- چهار گونه نشانهٔ امنیتی وجود دارد:

1. رمز ثابت
2. رمز پویا با استفاده از الگوریتم متقارن
3. رمز پویا با استفاده از الگوریتم نامتقارن
4. پرسش و پاسخ

- در این نوشته منظور نوع دوم نشانه‌است.
- ساده ترین نوع نشانه نیاز به اتصال به کامپیوتر ندارد. مشتری اعداد را به وسیله صفحه کلیدی که روی صفحه نمایش وجود دارد وارد می‌کند و سپس شماره شناسایی شخصی یا PIN code برای ورود به نشانه را زده وارد می‌شود. هرچند قطع شدن از سرور احراز هویت باعث می‌شود که نشانه‌ها در مقابل حملات میانی آسیب پذیر باشند.
- بعضی از نشانه‌ها به وسیله اتصالات بی سیم به کامپیوتر وصل می‌شوند، مانند بلوتوث .این نوع نشانه‌ها دنباله‌ای از کلید را به مشتری محلی یا نزدیک ترین نقطه دسترسی انتقال می‌دهند.
- نوع دیگر نشانه که امروز خیلی کاربرد وسیعی دارد، تلفن‌های همراه هستند که از ارتباطات در سطح کانال‌های out-of-band مثل صدا، پیام کوتاه، USSDو... استفاده می‌کند. این نوع نشانه نیز همانند نشانه‌های غیر متصل فیزیکی (نوع اول) در مقابل حملات میانی آسیب پذیر هستند.

امضای دیجیتال

• امضای دیجیتال به اندازه امضای دستی قابل اطمینان است. برای ساخت امضای دیجیتال نیاز به یک کلید خصوصی است که فقط خود فرد مجاز آن را می داند. نشانه‌ها با انجام عملیات تولید مطمئن و ذخیره کلید خصوصی امضای دیجیتال را امن می‌کنند. به این ترتیب برای احراز هویت قابل استفاده‌است. چون همانطور که گفته شد کلید خصوصی نشانه‌ای بر شخصیت فرد و یگانه بودن آن است. نشانه‌هایی که برای احراز هویت استفاده می‌شوند باید یک شماره خاص و یکتا داشته باشند. تمام روش‌های نشانه برای امضای دیجیتال به مسائل و قوانین ملیتی مناسب نیستند. نشانه‌هایی کهصفحه کلید ندارند یا از **اینترفیس‌های**)به انگلیسی (Interface :دیگری استفاده می‌کنند برای سناریو امضا مناسب نیستند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- بعضی از نشانه‌های امنیتی هم به صورت سخت افزاری و هم به صورت نرم‌افزاری در دسترس هستند. اگر فردی به این دو نوع نشانه امنیتی نگاه کند، از لحاظ ساختاری یکسان به نظر می‌رسند ولی در توابع یک سری تفاوت‌هایی با هم دارند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **نشانه غیرمتصل(Disconnected)**
- نشانه مورد نظر هیچ گونه اتصال فیزیکی و منطقی با کامپیوتر مشتری ندارد. به طور معمول به دستگاه ورودی خاصی نیاز ندارند. در عوض یک صفحه نمایش داخل خود دارند که داده‌های احراز هویت به وسیله آن نمایش داده می‌شود و کاربر به صورت دستی اطلاعات را با صفحه کلید وارد می‌کند. این نوع نشانه (معمولاً همراه یک رمز عبور) برای احراز هویت در تشخیص افراد به صورت بر خط بیشتر مورد استفاده قرار می‌گیرد.

یک نشانه غیر متصل

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **نشانه متصل(Connected)**

  - این نوع نشانه باید حتماً به صورت فیزیکی به کامپیوتر مشتری متصل گردد. نشانه‌ها در این دسته به طور اتوماتیک اطلاعات احراز هویت را به کامپیوتر مشتری در همان اولین ارتباط منتقل می‌کند، به جز اطلاعاتی که باید به طور دستی توسط کاربر داده شود. برای استفاده از این نوع نشانه باید دستگاه ورودی مناسبی روی سیستم نصب شود. معمول ترین نوع از نشانه‌های متصل، کارت‌های هوشمند و نشانه USB است که به ترتیب نیاز به دستگاه کارت خوانکارت هوشمند و پورت USB دارند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **کارت هوشمند**

- بسیاری از نشانه‌های متصل از تکنولوژی کارت هوشمند استفاده می‌کنند. کارت هوشمند می‌تواند خیلی ارزان و شامل مکانیزم‌های امنیتی مطمئن باشد. (همانند آن‌هایی که توسط مؤسسه‌های مالی استفاده می‌گردد، مثل دسته چک) عملکرد محاسباتی کارت هوشمند اغغلب محدود است و آن به دلیل توان مصرفی بسیار کم آن هاست.

ضرورت استفاده از پروتکل SSL

- بسیاری از افراد اطلاعات مورد نیاز خود را در طول روز از طریق اینترنت دریافت و ارسال می نمایند. برخی از این اطلاعات محرمانه نبوده و اهمیت چندانی ندارد.

به عنوان مثال: آگهی فروش سهام یک شرکت مطلب محرمانه ای نیست.

- اما برخلاف این اطلاعات، اطلاعاتی وجود دارند که بسیار قابل اهمیت و محرمانه هستند.

به عنوان مثال رمز حسابهای بانکی از این قبیل اطلاعات است.

ضرورت استفاده از پروتکل SSL

- درصورتیکه در هنگام انتقال چنین اطلاعاتی از پروتکل امنیتی استفاده ننمائیم، این احتمال وجـود دارد کـه اطلاعـات بدون آگاهی خودمان به سرقت رفته و مورد سوء استفاده قرار گیرند.

- اینجاست که بحث امنیت اطلاعات انتقالی و پروتکل های امنیتی مثل SSL مطرح می‌شود.

پروتکل SSL

- SSL یا Secure Socket Layer ،یکی از پروتکل‌های انتقال اطلاعات در وب و بین یک مرورگر و یک سرور است و انتقال اطلاعات را به صورت امن تضمین می نماید.
- این پروتکل که رایجترین پروتکل انتقال امن اطلاعات در وب است، توسط کمپانی Netscape تهیه شد و پس از مدتی علاوه بر مرورگر Netscape، توسط مرورگرIE نیز مورد استفاده قرار گرفت.
- اکنون تقریباً تمام مرورگرهای استاندارد از جمله فایر فاکس، اینترنت اکسپلورر، اپرا، گوگل کروم و سافاری آن را پشتیبانی می کنند.

عملکرد پروتکل SSL

- هنگام استفاده از SSL، مرورگر از public key موجود در خود استفاده کرده و اطلاعات را کد می نماید و سپس به سرور می فرستد. آنگاه سرور با استفاده از private key خود، اطلاعاتی را که دریافت نموده است رمز گشائی (Decode) می نماید.
- از آنجا که کلید خصوصی تنها در سرور نصب شده است، تقریباً غیر ممکن است که در بین راه اطلاعات انتقالی رمزگشائی و مشاهده شوند.

مکانیزم‌های تشکیل دهنده پروتکل SSL

❖مکانیزم های تشکیل دهنده SSL عبارتند از:

1. تایید هویت سرویس دهنده
2. تایید هویت سرویس گیرنده
3. ارتباطات رمز شده

اجزای پروتکل SSL

❖ پروتکل SSL دارای دو زیرپروتکل تحت عناوین زیر می باشد:

1. SSL Record Protocol : که نوع قالب بندی داده های ارسالی را تعیین می‌کند.
2. SSL Handshake Protocol : که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده ها میان سرویس دهنده و سرویس گیرنده را فراهم می‌سازد.

مزایای بخش بندی پروتکل SSL به دو زیر پروتکل

1. در ابتدای کار و طی مراحل اولیه ارتباط دست تکانی (Handshake) هویت سرویس دهنده برای سرویس گیرنده مشخص می گردد.

2. در همان ابتدای شروع مبادلات، سرویس دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می کنند.

به دو زیر پروتکل SSLمزایای بخش بندی پروتکل

3. در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس دهنده احراز می گردد.
4. در صورت استفاده از تکنیک های رمزنگاری مبتنی بر کلید عمومی، می‌توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.
5. ارتباطات رمزنگاری می شود.

پروتکل HTTPS

- در حال حاضر بسیاری از وب سایت ها علاوه بر پروتکل معمول HTTP از SSL نیز حمایت می کننـد و بـرای دسترسـی امن به اطلاعات وب‌سایت های مذکور می توان از HTTPS استفاده کرد.

- پروتکل HTTP-S همان Secure HTTP است و از پروتکل SSL برای انتقال اطلاعات استفاده می‌کند.

پروتکل HTTPS

در موارد زیر از پروتکل Https استفاده می‌شود:

- بانک ها
- فروشگاه های الکترونیکی
- Mail Serverها
- و کلیه سایت هایی با اطلاعات مهم و محرمانه کار می‌کنند.

پروتکل HTTPS

- قابل ذکر است که پروتکلHTTP به صورت پیش فرض از پورت ۸۰ استفاده می کند در حالی کـه پروتکـل HTTPS بـه صورت پیش فرض از پورت ۴۴۳ استفاده می کند. به عبارت دیگر این دو پروتکل دو مجرای ارتباطی کاملاً مجزا دارند.

- تبدیل کدها (رمزگذاری و رمز گشایی) در مبدا و مقصد زمانی را به خود اختصاص می‌دهند. بنـابراین سـرعت HTTPS از HTTP کمتر است.

پروتکل HTTPS

- وبسایت‌هایی که از پروتکل امن SSL جهت رمزگذاری داده‌ها استفاده می‌کننـد، از طریـق پروتکـل (HTTPS) بـه جـای حالت عادی و غیر امن آن یعنی HTTP با سرویس گیرنده‌ها ارتباط برقرار می‌کنند.

- در مرورگرها، اینگونه وبسایت‌ها معمولاً با علامت قفل سبز (به معنای ارتباط امن سالم) نشان داده می‌شوند.

❖ مشخصه های مهم یک فایروال

1. توانایی ثبت و اخطار
2. بازدید حجم بالایی از بسته های اطلاعات
3. سادگی پیکربندی
4. امنیت و افزونگی فایروال

انواع فایروال

- . فایروالهای سطح مدار (Circuit-Level)
- 2. فایروالهای پروکسی سرور
- فیلترهای Nosstateful packet
- فیلترهای Stateful Packet
- فایروالهای شخصی

❖ موقعیت یابی برای فایروال

موقعیت و محل نصب از لحاظ توپولوژیکی

قابلیت دسترسی و نواحی امنیتی

مسیریابی نامتقارن

فایروال‌های لایه‌ای

❖ چه نوع فایروال هائی وجود دارد ؟

سخت افزاری

نرم افزاری

امنیت مودم

- چگونه امنیت مودم وایرلس رو افزایش بدیم؟

1: تغییر پسورد

2: تعیین رمز برای مودم های وایرلس

3: مخفی کردن و روش SSID

4: فیلتر کردن ابزار ها به کمک آدرس

5: استفاده از قفل شبکه

6: نصب نرم افزار CISCO NETWORK Magic

7: استفاده فایروال

8: خاموش کردن وایرلس کل مودم

امنیت دانلود اطلاعات

- امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم های اطلاعاتی از فعالیت های غیر مجاز که این فعالیت ها عبارتند از :
- دسترسی ، استفاده ، افشاء ، خواندن ،نسخه برداری، خراب کردن، تغییر، دستکاری ..
- واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشتباه به جای هم بکار برده می‌شود. اگر چه اینها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آنها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده‌اند دارد..

IDMامنیت دانلود اطلاعات بوسیله

- IDM: internet download mamenger

- Internet Download Managerیا به اختصار « «IDMنرم افزاری پیشرفته برای مدیریت دانلود است که با سیستم هوشمند خود مدیریت کردن فایل‌های دانلود را آسان‌تر می‌سازد، این برنامه با تکنولوژی جدید خود باعث سرعت بخشیدن به امر دانلود کردن فایل‌ها می‌شود و طبق گفته شرکت سازنده تا 5 برابر سریعتر از حالت معمولی می‌تواند دانلود کند.

قابلیت‌های کلیدی نرم افزار Internet Download Manager

- ***افزایش سرعت دانلود تا 5 برابر توسط سیستم هوشمند «تقسیم بندی پویا».***
- ***- قابلیت Resumeجهت قطع و ادامه دانلود در زمان دیگر بدون از دست داده اطلاعات دانلود شده.***
- ***- پشتیبانی از تمامی مرورگرها و برنامه‌های رایج در بازار.***
- ***- قابلیت Video Grabberجهت دانلود فایل‌های تصویری در سایت‌ها.***
- ***- قابلیت خودکار چک کردن فایل‌ها توسط ضد ویروس‌ها.***
- ***- قابلیت Site Grabberجهت دانلود تمامی محتویات یک سایت.- قابلیت دانلود چندگانه فایل‌ها.***
- ***- قابلیت زمان بندی پیشرفته برای مدیریت دانلودها.***
- ***- قابلیت Speed Limiterجهت محدود نمودن سرعت دانلود.***
- ***- پشتیبانی از زبان‌ها مختلف از جمله زبان شیرین فارسی.***

نکات قابل توجه:

- **1: ترجیهاً از دانلود کردن چند فایل به طور همزمان خودداری نمایید.**

2: از قطعه بندی بیش از حد فایل‌ها (حتی در این برنامه و در برنامه‌های دیگر) خودداری کنید.

- **3: استفاده کردن از این برنامه جهت دانلود نمودن مطمئن فایل‌های خود بسیار پیشنهاد می‌شود.**

چگونه متوجه شویم مودم مشغول فعالیت است؟

- زمانی که مودم در حال برقراری اتصال است صداهای جیغ مانندی از آن به گوش خواهد رسید. اینها سیگنالهای دیجیتالی هستند که از طرف کامپیوتر مبدا (درخواست کننده برقراری اتصال) ارسال شده و به صداهای قابل شنود Modulateمی شوند (به سیگنالهای آنالوگ صدا تبدیل می شوند). مودم برای نمایش رقم 1 یک Toneقویتر (صدای بلندتر) و برای نمایش رقم 0 یک Tone ضعیفتر می فرستد.

چه اقداماتی را انجام دهیم تا مودم ADSL امن داشته باشیم

ا جازه ی کنترل از راه دور به مسیریاب را غیر فعال کنید .

- نام کاربری و رمز مسیریاب را عوض کنید.
- فایروال مسیریاب خود را فعال کنید .
- شبکه ی بی سیم مسیریاب خود را ایمن کنید.
- .روی شبکه ی بی سیم خود رمز بگذارید
- باشید. WPSمراقب
- از شیوه ی کنترل دسترسی استفاده کنید.
- شناسه ی دستگاه یا نام شبکه ی بی سیم را تغییر دهید
- به روز کردن سفت افزار مسیریاب.

مودم چیست ؟

- Modemمخفف کلمات Modulator/Demodulatorبوده و به شما امکان می دهد که کامپیوتر خود را به یک خط تلفن استاندارد متصل کنید به طوری که قادر به ارسال یا دریافت داده های الکترونیکی باشید. در واقع استفاده از مودم کلید اصلی ورود به دنیای اینترنت و وب جهان شمول (www=world wide web)، سرویسهای آنلاین تجاری، ایمیل، و سیستمهای بُرد بولتین (BBSesمی باشد.

انواع مودم:

- **1. مودم خارجی:**
- **در بین مودم های ذکر شده، نصب و راه اندازی مودم خارجی ساده تر است. زیرا برای نصب آن نیاز به باز کردن درب کیس کامپیوتر نیست. مودمهای خارجی منبع تغذیه مخصوص خود را داشته و از طریق کابلی به پورت سریال کامپیوتر متصل می شوند. خط تلفن هم به داخل سوکتی واقع در پشت مودم متصل می شود.**

- **2. مودم داخلی:**
- **زمانی که اقدام به خرید کامپیوتر آماده می کنید، معمولا مودم داخلی در آن نصب است. لذا مودم های داخلی اغلب با سیستم کامپیوتری تطابق بیشتری داشته و نیاز به توجه خاصی ندارند. زمانی که یک برنامه اتصال به اینترنت را در کامپیوتر خود اجرا می کنید مودم داخلی فعال می شود و زمانی که از آن برنامه خارج می شوید مودم خاموش می شود. این راحتی استفاده، مودم داخلی را مخصوصا برای کاربران مبتدی به ابزاری مفید تبدیل می کند.**
- **مودمهای داخلی معمولا ارزانتر از مودمهای خارجی هستند ولی اختلاف قیمت معمولا ناچیز است.**
- **مهمترین مشکل استفاده از مودمهای داخلی مکان قرارگیری آنهاست: آنها درون کیس کامپیوتر هستند. لذا زمانی که می خواهید یک مودم داخلی را جایگزین کنید بایستی درب Caseکامپیوتر را باز کرده و مودم را تعویض کنید.**

مودم‌های دیجیتال:

- **این مودم‌ها برای اتصال به خطوط دیجیتال تلفن شهری استفاده می‌شوند، و کار تبدیل اطلاعات دیجیتال خطوط تلفن را به اطلاعات قابل فهم برای رایانه (و برعکس) را انجام می‌دهند. هزینه این اتصال نسبت به هزینه خطوط آنالوگ بالاتر است و بالاترین نرخ انتقال اطلاعات در این مودم‌ها برابر 64 کیلوبیت در ثانیه است.**