SSL ، امنیت دیجیتالی

طاهر خرمالی

فهرست مطالب

۱- مقدمه

امضای دیجیتال و امنیت دیجیتالی چیست ۴
گواهینامه دیجیتالی چیست و چرا ما به یکی نیاز داریم؟.....۵
ثبت نام برای یک گواهینامه دیجیتالی ۶
پخش کردن گواهینامه دیجیتالی ۶
انواع مختلف گواهینامه دیجیتالی ۷
سطوح مختلف گواهینامه های الکترونیکی ۷
امضای دیجیتالی از دید برنامه نویسی ۸
چگونه یک امضای دیجیتالی درست کنیم؟.....۹
نحوه عملکرد یک امضای دیجیتال ۱۱
نحوه ایجاد و استفاده از کلید ها ۱۲
حملات ممکن علیه امضاء های دیجیتالی ۱۲
مرکز صدور گواه ینامه چیست؟ ۱۳
رمزنگاری چیست؟ ۱۴
اهداف CA ۱۵
نکاتی در مورد گواهینامه ها ۱۶
تشخیص هویت از طریق امضای دیجیتالی ۱۶
امضای دیجتالی زیربنای امنیت تبادلات الکترونیکی.....۱۷
گفتگو با دبیر کمیته IT دفتر مطالعات فناوری ریاست جمهوری.....۱۸

۲- SSL چیست؟

۲-۱ InstantSSL چیست؟ ۲۵
۲-۲ تکنولوژی پیشرفته تایید کردن (Authentication).....۲۵
۲-۳ دسترسی آنلاین به پروفایل تجاری تان ۲۵

۳- مفاهیم رمز گذاری

۳-۱ معرفی و اصطلاحات ۲۵
۳-۲ معرفی الگوریتمهای رمزنگاری ۲۷

۳-۳ رمزنگاری کلید – عمومی ۲۸
۳-۴ مقدار Hash ۲۹
۳-۵ آیا شما معتبر هستید ؟ ۳۰
۳-۶ سیستمهای کلید متقارن ۳۳
۳-۷ سیستمهای کلید نامتقارن ۳۵
۴- ساختار و روند آغازین پایه گذاری یک ارتباط امن
۴-۱ پروتکل های مشابه ۴۱
۵- مفهوم گواهینامه در پروتکلSSL
۵-۱ مراکز صدور گواهینامه ۴۲
۵-۲ مراحل کلی برقراری و ایجاد ارتباط امن در وب ۴۳
۵-۳ نکاتی در مورد گواهینامه ها ۴۴
۵-۴ تشخیص هویت ۴۵
۶ – مشکلات و معایب SSL
۶-۱ مشکل امنیتی در SSL ۶۰
۶-۲ مشکلات تجارت الکترونیکی در ایران ۶۰
ضمیمه ۱ : پیاده سازی SSL در Windows 2000 Server..... ۶۲
ضمیمه ۲ : پراکسی (Proxy)..... ۶۶
واژه نامه ۷۷
فهرست منابع ۷۸

امضای دیجیتال و امنیت دیجیتالی چیست ؟

امضای [[دیجیتال]] برای فایل های اطلاعاتی همان کار را انجام می دهد که امضای شما بر روی سند کاغذی انجام می دهد.امضای دیجیتال و امضای دس تنو یس هر دو متکی بر این واقعیت هستند که پیداکردن دو نفر با یک امضا تقریباً غیرممکن است. باامضای دیجیتال اصل بودن و صداقت یک پیغام یا سند و یا فایل اطلاعاتی تضمین میشود. به منظور ایجاد امضای دیجیتال از یک [[الگوریتم ریاضی]] به منظور ترکیب اطلاعات در یک کلید با [[اطلاعات]] پیام ، استفاده می شود . ماحصل عملیات ، تولید رشته ای مشتمل بر مجموعه ای از حروف و اعداد است .یک امضا ی دیجیتال صرفا" به شما نخواهد گفت که " این شخص یک پیام را نوشته است " بلکه در بردارنده این مفهوم مهم است که : "این شخص این پیام را نوشته است " .

از نگاهی دیگر یک گواه ینامه دیجیتالی یک فایل دیجیتالی است که به صورت رمزگذاری شده ای حاوی اطلاعاتی از قبیل کلید عمومی و سایر اطلاعات خود دارنده است. دارنده می تواند یک شخص، یک شرکت، یک سایت و یا یک نرم افزار باشد. مانند یک گواه ینامه رانندگی که عکس صاحب خود را به همراه سایر اطلاعات در مورد دارنده آن، شامل می شود، یک گواه ینامه دیجیتالی نیز یک کلید عمومی را به اطلاعات ی در مورد دارنده آن متصل می کند.در کلام دیگر، گواه ینامه دیجیتالی آلیس، تصدیق م ی کند که کلید عمومی به او و تنها او تعلق دارد. به همراه کلید عمومی، یک گواه ینامه دیجیتالی حاوی اطلاعاتی در مورد شخص حقیقی یا حقوقی دارنده آن می باشد، که برای شناسایی دارنده، و (بر این اساس که گواه ینامه ها محدود می باشند)، تاریخ ابطال آنرا نمایش می دهد.

دفاتر ثانویه مطمئن صادر کننده گواه ینامه، هویت شخص دارنده گواه ینامه را قبل از آنکه تصدیق کنند، چک می کنند .بخاطر اینکه گواه ینامه دیجیتالی اکنون یک فایل اطلاعاتی کوچک است، اصل بودن آن توسط امضا ی دیجیتالی خودش قابل بررس ی است لذا به همان صورتی که یک امضای دیجیتالی را تایید می کنیم به همان صورت از صحت امضای دیجیتالی به اصل بودن گواه ینامه پی خواه یم برد.

گواهینامه دیجیتالی چیست و چرا ما به یکی نیاز داریم؟

اجازه دهید برای پاسخ به سوال فوق ، سوالات دیگری را مطرح کنیم ! • برای تشخیص و تائید هویت فرد ارسال کننده یک نامه الکترونیکی از چه مکانیزم هائی استفاده می شود؟ • فرض کنید یک نامه الکترونیکی از یکی از دوستان خود دریافت داشته اید که از شما درخواست خاصی را می نماید ، پس از مطالعه پیام برای شما دو سوال متفاوت مطرح می گردد : الف) آیا این نامه را واقعا" وی ارسال نموده است ؟ ب) آیا محتوای نامه ارسالی واقعی است و وی دقیقا" همین درخواست را داشته است ؟ • آیا وجود هر نامه الکترونیکی در صندوق پستی ، نشاندهنده صحت محتوا و تائید هویت فرد ارسال کننده آن است ؟ سوءاستفاده از آدرس های Email برای مهاجمان و ویروس ها به امری متداول تبدیل شده است و با توجه به نحوه عملکرد آنان در برخی موارد شناسائی هویت فرد ارسال کننده یک پیام بسیار مشکل و گاها " غیرممکن است . تشخیص غیرجعلی بودن نامه های الکترونیکی در فعالیت های تجاری و بازرگانی دارای اهمیت فراوانی است . یک نامه الکترونیکی شامل یک امضای دیجیتال، نشاندهنده این موضوع است که محتوای پیام از زمان ارسال تا زمانی که به دست شما رسیده است ، تغییر نکرده است . در صورت بروز هر گونه تغییر در محتوای نامه ، امضای دیجیتال همراه آن از درجه اعتبار ساقط می شود .

یک گواه ینامه دیجیتالی یک فایل دیجیتالی است که به صورت رمزگذار ی شده ا ی حاوی اطلاعاتی از قبیل کلید عمومی و سایر اطلاعات دارنده خود است. دارنده می تواند یک شخص، یک شرکت، یک سایت و یا یک نرم افزار باشد. مانند یک گواه ینامه رانندگی که عکس صاحب خود را به همراه سایر اطلاعات در مورد دارنده آن، شامل می شود، یک گواه ینامه دیجیتالی نیز یک کلید عمومی را به اطلاعاتی در مورد دارنده آن متصل می کند.

در کلام دیگر، گواه ینامه دیجیتالی آلیس، تصدیق می کند که کلید عمومی به او و تنها او تعلق دارد. به همراه کلید عمومی، یک گواه ینامه دیجیتالی حاوی اطلاعاتی در مورد شخص حقیقی یا حقوقی دارنده آن می باشد، که برا ی شناسا یی دارنده، و (بر ا ین اساس که گواه ینامه ها محدود می باشند)، تاریخ ابطال آنرا نمایش می دهد.

دفاتر ثانویه مطمئن صادر کننده گواه ینامه، هویت شخص دارنده گواه ینامه را قبل از آنکه تصدیق کنند، چک می کنند .بخاطر اینکه گواه ینامه دیجیتالی اکنون یک فایل اطلاعاتی کوچک است، اصل بودن آن توسط امضا ی دیجیتالی خودش قابل بررس ی است لذا به همان صورتی که یک امضای دیجیتالی را تایید می کنیم به همان صورت از صحت امضای دیجیتالی به اصل بودن گواه ینامه پی خواه یم برد.

ثبت نام برای یک گواهینامه دیجیتالی

کاربران می توانند از طریق وب برای یک گواه ینامه دیجیتالی ثبت نام کنند. پس از کامل شدن فرمهای مورد نیاز، مرورگر اینترت کاربر یک جفت کلید عمومی درست می کند. یکی از کلید عمومی به دفاتر صدور گواه ینامه برای درج در مشخصات دارنده آن ارسال می شود .درحالیکه کلید خصوصی کاربر بر روی کامپیوتر او در جایی امن (هارد دیسک، فلاپی درایو و ...) نگهداری خواهد شد.

دفاتر صدور گواه ینامه در ابتدا ملزم به تایید اطلاعات ارسال شده توسط کلید عموم ی کاربر می باشند. اینکار از جا زدن کسی به جای کس دیگر و احتمال وقوع تبادلات نامشروع و غیر قانونی جلوگیری می کند.
اگر اطلاعات ارسال شده درست باشد، دفتر صادر کننده گواه ینامه، یک گواه ینامه دیجیتالی برای متقاضی خود صادر می کند. بمحض صدور، دفتر صادر کننده گواه ینامه امضای دیجیتالی را در یک بایگانی عمومی نگهداری می کند.

پخش کردن گواهینامه دیجیتالی

در حالیکه گواه ینامه دیجیتالی در یک بایگانی عمومی ذخیره شده است نیز، می تواند با استفاده از امضای دیجیتالی پخش گردد. به طور مثال زمانیکه آلیس نامه ای را برای باب به صورت دیجیتالی امضا می کند، او همچنین گواه ینامه خود را به آن نامه پیوست می کند .
لذا همزمان با دریافت نامه دیجیتالی باب میتواند معتبر بودن گواه ینامه آلیس را نیز بررسی کند. اگر با موفقیت تایید شد، هم اکنون باب کلید عمومی آلیس را دارد و نیز میتواند اعتبار نامه ارسالی از طرف آلیس را بررسی کند.

انواع مختلف گواهینامه دیجیتالی

بر حسب نوع استفاده از گواه‌ینامه دیجیتالی، چند نمونه مختلف از آن موجود می باشد.

- شخصی: قابل استفاده توسط اشخاص حقیقی برا ی امضا ی ایمیل و تبادلات مالی.
- سازمان ها: قابل استفاده توسط اشخاص حقوقی برای شناساندن کارمندان برای ایمیل های محفوظ و تبادلات تحت اینترنت.
- سرور: برای اثبات مالکیت یک دامین اینترنتی.
- تولید کنندگان: برای اثبات حق تالیف و حفظ حقوق آن برای نشر برنامه نرم افزاری.

سطوح مختلف گواهینامه های الکترونیکی

گواهینامه های دیجیتالی در سطوح مختلفی بسته به میزان و سطح اطمینان خواسته شده از طرف متقاضی، توسط دفاتر صدور گواه‌ینامه موجود می باشند. در زبان ساده هر چه سطح گواه‌ینامه بالاتر باشد، به میزان بیشتری دارنده آنرا تا ییید م ی کند. یک گواه‌ینامه سطح بالا میتواند به این معنی باشد که گواه‌ینامه م ی تواند برا ی کارها ی حساس تری مانند بانکداری آنلاین و معرفی هویت یک نفر برای تبادلات مالی و تجارت الکترونیکی، مورد استفاده قرار بگیرد.

سطح گواه‌ینامه ارتباط نزدیکی با نوع گواه‌ینامه دارد. سطوح پا ییین شامل اطلاعات شخصی کمتری و یا بدون اطلاعات شخصی می باشند (به طور مثال فقط یک آدرس ایمیل). گواه‌ینامه های متعلق به چنین سطحی می توانند برای ارسال ایمیل حفاظت شده بکار بروند، در حالیکه برای اثبات گواهینامه یک موسسه و یا یک سازمان نیاز به اطلاعات بیشتری و در نتیجه سطح بالاتری از گواه‌ینامه است.

امضای دیجیتالی از دید برنامه نویسی

در یک امضای دیجیتالی سه دسته اطلاعات وجود دارد: هویت تولید کننده نرم افزار، هویت منبع تایید کننده (سازمانی که امضاء را صادر کرده) و یک عدد رمز برا ی تایید این مطلب که محتویات نرم افزار دستکاری نشده است.

اگر می خواه ید برای وب محتویات فعال بنویسید باید یک گواه ینامه کد تعیین اعتبار برای خود دست و پا کنید تا بتوانید برای نرم افزار های خود امضای دیجیتالی بگیرید . اگر فقط برای اینترنت برنامه می نویسید نیازی به این مراحل ندارید چون سطح امنیتی در آنها معمولا پایین است و نیازی به امضای دیجیتالی وجود ندارد.

اگر صرفاً برای شرکت خود نرم افزار می نویسید م ی توانید از گواه ینامه آن استفاده کنید. اما توصیه می شود خودتان هم این گواه ینامه را بگیرید.

با آن که شرکت های متعددی برای صدور گواه ینامه کد تع یین اعتبار وجود دارند، میکروسافت شرکت Verisign را توصیه می کند. برا ی کسب اطلاعات ب یشتر م ی توانید به سایت وب این شرکت که در زیر آمده است مراجعه کنید:

http://www.verisign.com/developers/index.html

هزینه دریافت این گواه ینامه ۲۰ دلار در سال و مراحل انجام آن بسیار ساده است:

۱- در سا یت مزبور، یک فرم پر کنید و در آن اطلاعات خواسته شده (از جمله اطلاعات مربوط به کارت اعتباری) را وارد کنید.

۲- شرکت Verisign کد شناسایی شما را با پست الکترون یک برایتان ارسال خواهد کرد.

۳- به صفحه نصب گواه ینامه رفته و کد شناسایی خود را وارد کنید. این کار با ید در همان کامپوتری که توسط آن کد شناسایی را گرفته اید، انجام شود.

۴- گواه ینامه به کامپوتر شما فرستاده خواهد شد.

هنگام ثبت گواه ینامه دو گزینه در اختیار دارید: ذخیره کردن آن در یک فایل یا در رجیستری ویندوز. توصیه می شود گواه ینامه خود را در یک فایل و روی دیسک ذخیره کنید تا بتوانید آن را از گزند نامحرمان حفظ کنید. در حقیقت، دو فایل به کامپ یوتر شما فرستاده می شود: یکی حاوی خود گواه ینامه (با پسوند SPC) و دیگری حاو ی کلید رمزبندی (با پسوند PVK).

امضای دیجیتالی: امضای دیجیتالی برای ایمیل و فایل های اطلاعاتی همان کاری را انجام میدهد که امضای شما بر روی یک سند کاغذی انجام می دهد.امضای دیجیتالی اصل بودن وصداقت یک پیغام یا سند و یا فایل اطلاعاتی را تضمین می کند.

چگونه یک امضای دیجیتالی درست کنیم؟

کنگره امریکا استفاده از امضاهای دیجیتال را تصویب کرد. این طرح هم اکنون باید در مجلس سنای امریکا تصویب شود. با تصویب این طرح، امضای دیجیتال رسمی می شود و می توان از آن برای امضای قرارداد ها و اسناد مالی درست مانند امضای معمولی استفاده کرد. استفاده از امضای دیجیتال به چه تجهیزاتی نیاز دارد؟

۱- یک دستگاه کامپیوتر
۲- اتصال به اینترنت
۳- نرم افزار مخصوص امضای دیجیتالی

بوجود آوردن یک امضای دیجیتالی مراحل محاسباتی پیچیده ای دارد. در حالیکه این مراحل توسط کامپوتر انجام می شود، درست کردن امضای دیجیتالی دیگر حتی از یک امضای دستی هم آسان تر است. مراحل زیر نشان دهنده اعمالی است که در حین ساخته شدن یک امضای دیجیتالی صورت می گیرد:

a) آلیس دکمه singرا در نرم افزار ایمیل خود کلیک میکند و یا فایلی را که نیاز به امضا دارد انتخاب می کند.

b) کامپیوتر آلیس رمزگذاری را محاسبه می کند. (پیغام به یک تابع عمومی جهت رمزگذاری برده می شود). این تابع توسط کلید خصوصی آلیس رمزگذاری شده است (در این حالت آنرا کلید امضا می خوانیم).

c) پیغام آلیس و امضای دیجیتالی آن برای باب ارسال می شود.

d) باب پیغام امضا شده رادریافت می کند. در آنجا مشخص شده است که پیغام امضا شده است، و نرم افزار ایمیل باب می داند که چگونه آن امضا را تایید کند.

d) کامپیوتر باب امضای دیجیتالی آلیس را توسط کلید عمومی آلیس رمزگشایی می کند.

e) کامپیوتر باب کد رمزگذاری را از امضای دیجیتالی استخراج می کند. سپس کامپیوتر باب کد رمزگذاری را که استخراج کرده است با کدی که با پیغام آلیس ارسال شده است مطابقت می کند.

f) اگر پیغام آلیس صحیح انتقال یافته باشد و در طول راه مورد دستبرد واقع نشده باشد هر دو کلید استخراج شده یکسان می باشند. اگر دو کد رمزگذاری که استخراج شده اند با یکدیگر مطابقت نداشته باشد صلاحیت نامه منتفی است.

g) اگر پیغام اصلی مورد سرقت قرار گرفته باشد کد رمزگذاری که در کامپیوتر باب استخراج می شود متفاوت خواهد بود و در این صورت کامپیوتر باب به او اطلاع خواهد داد.

نحوه عملکرد یک امضای دیجیتال

قبل از آشنایی با نحوه عملکرد یک امضا ی دیجیتال ، لازم است در ابتدا با برخ ی اصطلاحات مرتبط با این موضوع بیشتر آشنا شویم :

• کلیدها (Keys) . از کلیدها به منظور ایجاد امضاهای دیجیتال استفاده می گردد . برای هر امضای دیجیتال ، یک کلید عمومی و یک کلید خصوصی وجو د دارد : کلید خصوصی ، بخشی از کلید است که که شما از آن به منظور امضای یک پیام استفاده می نمائید . کلید خصوصی یک رمزعبور حفاظت شده بوده و نمی بایست آن را در اختیار دیگران قرار داد . کلید عمومی ، بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد . زمانی که کلید فوق برای یک حلقه کلید عموم ی (public key ring) و یا یک شخص خاص ارسال می گردد ، آنان با استفاده از آن قادر به بررس ی امضای شما خواهند بود .

• حلقه کلید (Key Ring) ، شامل کلید های عمومی است . یک حلقه کلید از کلید های عمومی افرادی که برای شما کلید مربوط به خود را ارسال نموده و یا کلیدهایی که از طریق یک سرویس دهنده کلید عمومی دریافت نموده اید، تشکیل می گردد . یک سرویس دهنده کلید عمومی شامل کلید افرادی است که امکان ارسال کلیدعموم ی در اختیار آنان گذاشته شده است .

• اثرانگشت : زمانی که یک کلید تائید م ی گردد ، در حقیقت منحصربفرد بودن مجموعه ای از حروف و اعداد که اثرانگشت یک کلید را شامل م ی شوند . تائید م ی گردد .

• گواهینامه های کلید : در زمان انتخاب یک کلید از رو ی یک حلقه کلید ، امکان مشاهده گواهینامه (مجوز) کلید وجود خواهد داشت . دراین رابطه می توان به اطلاعات متفاوتی نظیر صاحب کلید ، تاریخ ایجاد و اعتبار کلید دست یافت .

نحوه ایجاد و استفاده از کلید ها :

• تولید یک کلید با استفاده از نرم افزارهائ ی نظیر PGP اقتباس شده از کلمات Pretty Good Privacy)و یا GnuPG (اقتباس شده از کلمات GNU Privacy Guard)

• معرفی کلید تولید شده به سایر همکاران و افرادی که دارای کلید می باشند .

• ارسال کلید تولید شده به یک حلقه کلید عمومی تا سایر افراد قادر به بررسی و تائید امضای شما گردند .

• استفاده از امضای دیجیتال در زمان ارسال نامه های الکترونیکی . اکثر برنامه ها ی سرویس دهنده پست الکترونیکی دارای پتانسیلی به منظور امضاء یک پیام می باشند

حملات ممکن علیه امضاهای دیجیتالی

• حملهٔ Key-only – در این حمله، دشمن تنها کلید عمومی امضاءکننده را می‌داند و بنابراین فقط توانایی بررسی صحت امضاهای پیام‌هایی را که به وی داده شده‌اند، دارد.

• حملهٔ Known Signature – دشمن، کلید عمومی امضاءکننده را می‌داند و جفت‌های پیام/امضاء که به‌وسیلهٔ صاحب امضاء انتخاب و تولید شده است را دیده است. این حمله در عمل امکان‌پذیر است و بنابراین هر روش امضایی باید در مقابل آن امن باشد.

• حملهٔ Chosen Message – به دشمن اجازه داده می‌شود که از امضاءکننده بخواهد که تعدادی از پیام‌های به انتخاب او را امضاء کند. انتخاب این پیام‌ها ممکن است به امضاهای از قبل گرفته شده بستگی داشته باشد. این حمله در غالب حالات،

ممکن است غیرعملی به نظر برسد، اما با پیروی از قانون احتیاط، روش امضایی که در برابر آن ایمن است، ترجیح داده می‌شود.

• حملهٔ Man-in-the-middle – در این حمله، شخص از موقعیت استفاده کرده در هنگام مبادلهٔ کلید عمومی، کلید عمومی خود را جایگزین کرده و برای گیرنده می‌فرستد و بدین‌گونه می‌تواند به پیام‌ها دسترسی داشته باشد بدون اینکه فرستنده و گیرنده، مطلع باشند. در سیستم‌های کلید ـ عمومی (نامتقارن) اغلب مدیریت کلید مورد حمله قرار می‌گیرد تا الگوریتم رمزنگاری

مرکز صدور گواه‌ینامه چیست؟

مرکزی برای صدور گواه ینامه و تایید هویت سرویس گیرنده و سرویس دهنده می باشد و بدین صورت عمل می کند که پس از درخواست گواه ینامه از طرف کاربر، CA به آن دو کلید خصوصی و عمومی می دهد که کلید خصوصی در اختیار کاربر قرار می گیرد و باید در جای امنی ذخیره شود.CA با استفاده از کلید عمومی و مشخصات کاربر برای آن گواه ینامه ای صادر می کند ، که این گواه ینامه شامل مشخصات کاربر و تار یخ اعتبار آن و امضای صادر کننده گواه ینامه می باشد .

مرکز صدور گواه ینامه دارای بخش های مختلفی است که به توضیح هر کدام از آن ها می پردازیم.

۱- مرجع صدور گواه ینامه ریشه (Root CA) : این مرکز باید امنیت بالایی داشته باشد و کسی به کلید های خصوصی آن دسترسی پیدا نکند و به این علت وظیفه اعطا گواه ینامه را بهCA محول می کند .

۲- مرجع صدور گواه ینامه (CA) : این مرجع وظیفه اعطا گواه ینامه را به کاربران بعهده دارد و دارای گواه ینامه ای از سوی مرجع صدور گواه ینامه ریشه برای اطمینان کاربران می باشد .

۳- مرجع ثبت نام (RA) : این مرجع وظیفه ثبت درخواست گواه ینامه کاربر و اعلام آن بهCA و اعطا گواه ینامه را از CA به کاربر بعهده دارد .

پس از گرفتن کلید خصوصی وعمومی ،کاربر امکان رمزنگاری و امضا کردن متن ارسالی را پیدا می کند .
CA ها دارای یک لیستی به نام CRL می باشند که در آن لیست گواه ینامه هایی که کلید خصوصی آن ها لو رفته وجود دارد و آن را به صورت پی در پی به اطلاع کاربران می رساند.

رمزنگاری چیست؟

رمزنگاری عبارت است از بهم ریختگی اطلاعات به طور ی که برا ی کسی قابل فهم نباشد. در رمزنگاری کاربر با استفاده از کلید عمومی گیرنده، اطلاعات را رمز می کند و برای گیرنده اطلاعات ارسال می کند. گیرنده اطلاعات ،اطلاعات رمز شده را توسط کلید خصوصی رمزگشایی می کند و چون کلید خصوصی هر شخص فقط در اخت یار خودش است تنها همان فرد امکان رمزگشایی اطلاعات را دارد.

اهداف CA :

۱-تامین امنیت لازم در انجام معاملات و محیط های الکترونیکی و ترویج فرهنگ استفاده از هویت الکترونیکی است .

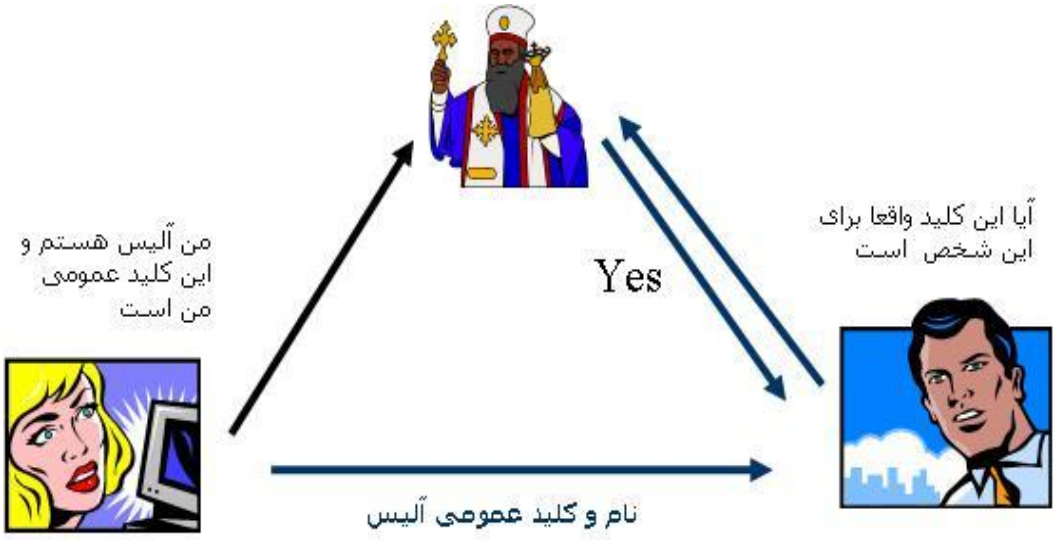
۲- تولید و ارائه گواهینامه دیجیتال برای تبادلات تجارت الکترونیکی C2B,B2B (در حوزه کالا و خدمات)

۳- تدوین آیین نامه ها و مقررات مربوط به مدیریت بر گواهی دیجیتال تولید و عرضه شده .

۴- ارائه خدمت به دفاتر ثبت گواهی دیجیتال (RA) و دفاتر خدمات گواهی دیجیتال در سراسر کشور .

۵- ارائه خدمات آموزشی برای استفاده از این فناوری در سراسر کشور .

با توجه به توضیحات داده شده و لزوم ایجاد CA در کشور به بررسی یکی از بزرگترین CA های جهان پرداخته می شود



تشخیص هویت از طریق امضای دیجیتالی :

یکی از مباحث مهم و اصولی در ارتباطات ایمن ، تشخیص هویت متقابل از هر دو طرف Client و Server می باشد. در یک ارتباط، هویت اصلی سرور برای کاربران و برعکس مشخص میشود زیرا در غیر این صورت هر سروری قادر به ایجاد اعتماد در کاربران خواهد بود . هر سرور باید دارای گواهینامه و امضای دیجیتالی باشد که این گواهینامه ، نشاندهنده هویت اصلی آن است و توسط شرکتهایی مانند Verisign و Thawte ارائه می گردد . در این گواهینامه الکترونیکی اطلاعاتی از قبیل : کلید عمومی (برای مخفی سازی اطلاعات) ، شماره سریال ، نام دامنه ، امضای دیجیتالی و تاریخ شروع و انقضای اعتبار گواهینامه درج می شود .

امضای دیجیتالی زیربنای امنیت تبادلات الکترونیکی

با توجه به توسعه روزافزون فناوری اطلاعات و در پی آن تجارت الکترونیکی و تغییر نمادهای فیزیکی به نمادهای الکترونیکی، ارسال و تبادل اطلاعات محرمانه الکترونیکی به ضرورتی اجتناب‌ناپذیر تبدیل شده است.

بنابراین مسائل حقوقی ناشی از تبادل الکترونیکی اطلاعات بایستی با قراردادهای مشخصی تنظیم شود. حوزه این مسائل، استانداردهای تبادل و ایمنی اطلاعات، نحوه اعتبارسنجی و رسمیت بخشیدن به پیام‌ها، نحوه دریافت و ارسال پیام، قوانین حاکم و سرانجام مسئله دلایل اثبات پیام را در بر می‌گیرند. به هر حال در روش ارسال پیام الکترونیکی دریافت‌کننده بایستی مطمئن شود که فرستنده همان فرد مورد نظر او بوده و از طرفی اطلاعات دریافتی پس از ارسال در بین راه تغییر نکرده باشد. برای حل این مشکل از امضای دیجیتالی در شبکه‌های الکترونیکی استفاده می‌شود. امروزه در اکثر کشورها امضای دیجیتالی به یک ضرورت تبدیل شده و حتی در کارت هوشمند شهروندان خود این رمز را درج می‌کنند از سوی دیگر جامعه بین‌المللی و همچنین انجمن قانونی بلژیک مجموعه قوانینی را ارائه کرده‌اند که باعث می‌شود امضاهای دیجیتال به صورت قانونی صورت پذیرد و عموما به صورت امضاهای مکتوب پذیرفته شود.

برای روشن شدن زوایای مختلف امضای دیجیتال خبرنگار گروه دانش و فناوری خراسان در گزارش پیش‌رو با دو تن از کارشناسان این حوزه، دکتر سیدعلی اکرمی‌فر، دبیر کمیته IT دفتر مطالعات فناوری ریاست جمهوری و دکتر محمود سلماسی‌زاده عضو هیئت علمی دانشگاه صنعتی شریف و مسئول کمیته علمی انجمن رمز ایران گفتگویی انجمن داده است که در ذیل می‌آید.

منظور از امضای دیجیتالی چیست؟

-امضای الکترونیکی یا دیجیتال مانند امضای سنتی نیست بلکه عددی بزرگ است که به صورت رمز و کد در آمده است. این عدد در حقیقت یک عدد انحصاری است و به فرد متقاضی، کد خاصی به عنوان امضای الکترونیک داده می‌شود.

آیا امضای الکترونیکی، فقط در تجارت الکترونیکی کاربرد دارد؟

-بخشی از آن مربوط به پرداخت و دریافت پول از طریق اینترنت می‌شود و در بخش دیگر به قراردادها، مرسولات الکترونیکی محرمانه و یا حتی شناخت طرف مقابل در شبکه مربوط می‌شود. یعنی تشخیص هویت فرد که برای شما چیزی ارسال کرده و یا شما خواهان دادن اطلاعاتی از سوی وی در شبکه اینترنت بوده‌اید. شناسایی هویت چیزی فراتر از تجارت است.

به طور کلی می‌توان گفت: امضای دیجیتال شماره یا عدد انحصاری محرمانه‌ای است که توسط مرکزی به هر فرد متقاضی تعلق می‌گیرد و آن عدد یا رمز مبنای تعاملات آن فرد در شبکه یا محیط سایبر می‌شود.

گفتگو با مسئول کمیته علمی انجمن رمز ایران

–چه مراکزی گواهی یا صدور امضای دیجیتال را بر عهده دارند و اصولا چرا صدور امضای دیجیتال نیاز به این مراکز دارد؟ و چگونه این مراکز ایجاد می‌شوند؟

-هم وزارت بازرگانی از طرف هیئت دولت موظف است امکان راه‌اندازی مراکز ایجاد و صدور گواهی دیجیتال که استفاده از امضای دیجیتال را عملی می‌کند فراهم کند که

هم اکنون این کار را می‌کند و هم بانک‌ها مشغول ایجاد یک مرکز صدور گواهی هستند.
برای این که یک امضای الکترونیکی از نظر قانونی به رسمیت شناخته شود تا هیچ یک از طرفین نسبت به اصالت و صحت اسناد مبادله شده از طریق اینترنت تردید نکنند و کسی منکر امضای دیجیتالی که ارائه کرده، نشود باید امضای دیجیتال گواهی شود.
مراکز گواهی امضای دیجیتال مشابه مراجع ثبت اسناد رسمی هستند و چون در محیط سایبر نیز احتمال تردید، انکار یا ادعای جعل نسبت به اسناد الکترونیکی وجود دارد پس باید در این فضا هم نهادها و مراجعی برای تضمین معاملات الکترونیکی باشند. این گواهی در واقع هویت امضاءکننده و صحت انتساب سند به وی را تایید می‌کند. مرجع گواهی می‌تواند هم یک نهاد دولتی یا زیرنظر دولت باشد و هم یک نهاد ملی و یا بین‌المللی. به هر حال الان مراکزی در اروپا هست که امیدواریم نکاتی برقرار شود تا آنها صحت گواهی ما را تایید کنند تا بتوانیم از سوی گواهی‌های صادره خود برای کاربردهای بین‌المللی هم استفاده کنیم.

استفاد از امضای دیجیتال تا چه حد امنیت تبادل اسناد مالی و محرمانه را تضمین می‌کند؟

امنیت هیچ وقت صددرصد نمی‌شود، این مقوله هم یک مسئله نسبی است و بستگی دارد چقدر برای آن می‌خواهید هزینه کنید و سندی را که می‌خواهید حفاظت کنید چه ارزشی دارد، با توجه به ارزشی که یک سند دارد برای مصونیت آن سرمایه‌گذاری می‌کنند. به هر حال امضای الکترونیکی بر خلاف امضای دست‌نویس از امنیت بیشتری برای مصون ماندن از جعل، دستکاری و تقلید توسط دیگران برخوردار است چون آگاهی یافتن از یک امضای الکترونیکی محرمانه کار بسیار دشواری است. باید توجه داشت که گسترش تجارت الکترونیکی مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع از تجارت است و این اطمینان باید از طریق تضمین امنیت تبادل داده‌های الکترونیکی صورت گیرد. هر چند با توسعه فناوری‌های نوین امنیت افزایش می‌یابد ولی همانطور که گفته شد هیچ‌گاه صددرصد نمی‌شود.

–آیا در کشور امکانات و فناوری‌های لازم برای صدور امضای دیجیتال وجود دارد؟ آیا از لحاظ حقوقی در این زمینه با مشکلی مواجه نیستیم؟

- از لحاظ امکانات نرم‌افزاری و سخت‌افزاری برای عملی کردن استفاده از امضای دیجیتال در کشور سرمایه‌گذاری شده وسازمان‌هایی مشغول پیاده‌سازی این سیستم‌ها هستند.

در قانون تجارت الکترونیکی امضای دیجیتال برای کاربردهای مشخصی به رسمیت شناخته شده است.
البته نیاز به آیین‌نامه‌هایی دارد که به تصویب نرسیده ولی در دست تهیه و تدوین برای تصویب است.

–معنی و مفهوم کلید عمومی و خصوصی در امضای الکترونیکی چیست؟

- منظور از کلید بخشی از سیستم یا الگوریتمی است که یک متن را رمزگذاری یا رمزگشایی می‌کند. کلید عمومی پیام را به صورت رمز در می‌آورد که شما می‌تواند کلید عمومی را در اختیار همگان و در معرض استفاده و دید عمومی قرار دهید.
مرکز گواهی برای آنها گواهینامه‌ای صادر می‌کند که صحت انتساب کلید عمومی را به هر شخص دارنده گواهی تایید می‌کند. کلید خصوصی هم کلید شخصی و منحصر به فردی است که محرمانه و در اختیار شخص است و فرد دیگری نمی‌تواند به آن دسترسی یابد.

امضای دیجیتال مبتنی بر روش‌های رمزنگاری از طریق کلیدهای عمومی و خصوصی است. یک متن یا پیام رمزنگاری شده بی‌مفهوم است و فقط کسی می‌تواند به معنی و مفهوم آن پی ببرد که دارای کلید خصوصی باشد.

– در حال حاضر از امضای دیجیتال در کشورهای دیگر چه استفاده‌هایی می‌شود؟

- در حال حاضر در دنیا در کشورهای متعددی از امضای دیجیتال در کاربردهای گوناگون استفاده می‌شود از صدور یک ایمیل گرفته تا نقل و انتقالات مالی و امضای اسناد تعهدآور. بنابراین حوزه کاربرد آن گسترده است. تاکنون مقتضیات قانونی آن در بیشتر نظام‌های حقوقی فراهم آمده است. این موضوع تا حدی است که در برخی ازکشورها مثل آلمان قانون مستقلی تحت عنوان قانون امضای الکترونیکی به تصویب رسیده است.

دکتر اکرمی‌فرد:
امضای دیجیتال شماره یا عدد انحصاری محرمانه‌ای است که مبنای تعاملات فرد در شبکه است

دکتر سلماسی‌زاده:
برای این که یک امضای الکترونیکی از نظر قانونی به رسمیت شناخته شود باید توسط مراکزی گواهی شود.

Secure Client Data &
Credit Card Protection

SSL "پروتکل ای است که توسط شرکت Netscape و برای رد و بدل کردن سند های خصوصی از طریق اینترنت توسعه یافته است .
یک کلید خصوصی برای به رمز در آوردن اطلاعاتی که بر روی یک ارتباط منتقل می شوند استفاده می نماید.
هر دو مرورگر Internet Explorer و Netscape Navigator { و امروزه تمام مرورگر های مدرن }
ازاین پروتکل پشتیبانی مینمایند. همچنین بسیاری از وب سایت ها برای فراهم کردن بستری مناسب جهت حفظ کردن اطلاعات محرمانه کاربران (مانند شماره کارت

اعتباری) از این پروتکل استفاده می نمایند. طبق آنچه در استاندارد آمده است ، URL هایی که نیاز به یک ارتباط از نوع SSL دارند با https: به جای http: شروع می شوند.

پروتکل دیگری که برای انتقال اطلاعات به صورت امن بر روی شبکه جهانی وب وجود دارد ، پروتکل ای است به نام Secure HTTP یا S-HTTP ، در حالیکه SSL یک ارتباط امن میان Client و Server ایجاد می کند تا هر اطلاعاتی که بر روی آن منتقل می شود امن باشد ، S-HTTP برای این طراحی شده است تا طبق آن پیام های منفرد به طور امن منتقل شوند .بنابراین این دو تکنولوژی قبل از آنکه دو تکنولوژی رقیب باشند ،[۱] دو تکنولوژی مکمل هستند. هر دو این پروتکل ها به عنوان استاندارد از سوی IETF پذیرفته شده اند.“

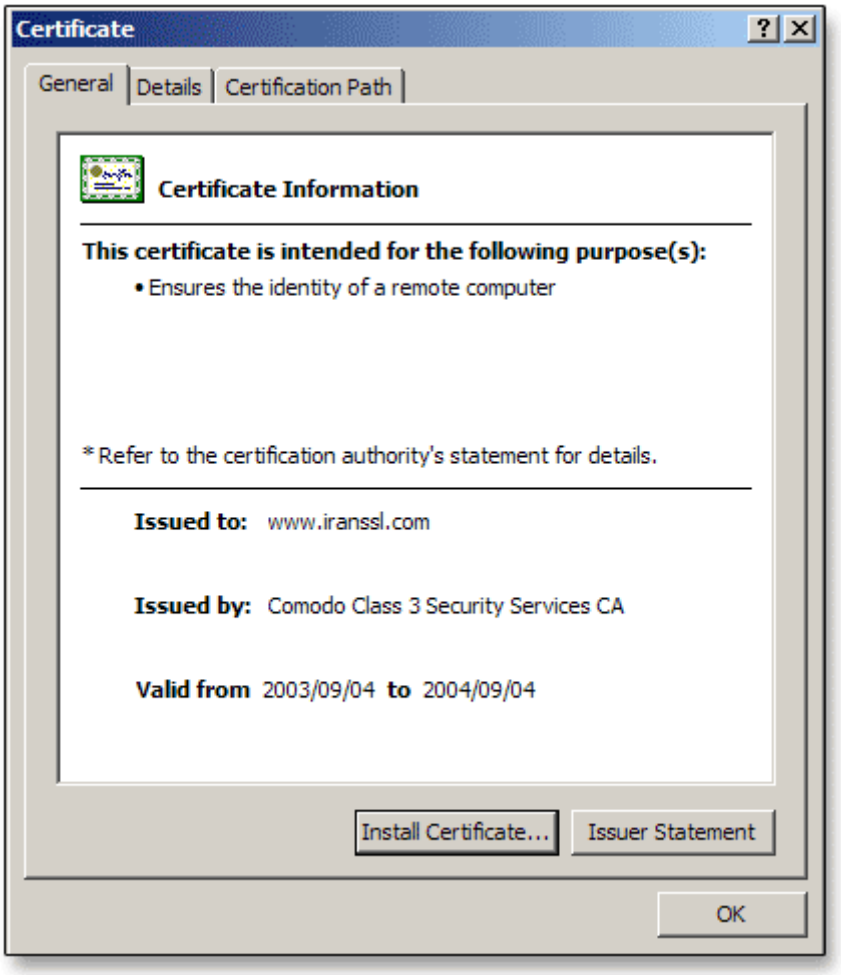
توجه داشته باشید که SSL یک پروتکل مستقل از لایه برنامه است (Application Independent) ، بنابراین پروتکل هایی مانند HTTP، FTP و Telnet قابلیت استفاده از آن را دارند. با این وجود SSL بروی پروتکل ها ی HTTP، FTP و IPSec بهینه شده است.

۲– SSL چیست؟

پروتکل (Socket Secure Layer) SSL ، یک استاندارد وب برا ی کدکردن اطلاعات بین کاربر و وب سا یت است. اطلاعاتی که توسط یک اتصال SSL مبادله می شوند بصورت کد شده ارسال م ی شوند و بد ین ترتیب اطلاعات مبادله شده از دزد یده شدن یا استراق سمع محافظت می شوند. SSL برای شرکتها و مشتریان این امکان را فراهم می کند که بتوانند ، با اطم ینان اطلاعات خصوصی شان را مانند شماره کارت اعتباری، به یک وب سایت بطور محرمانه ارسال کنند . برای برقراری یک اتصال SSL به Web Server Certificateها نیاز می باشد. در تعریفی دیگر SSL اینگونه بیان شده , Secure Socket Layerیا همان SSL یک تکنولوژی استاندارد و به ثبت رسیده برای تامین ارتباطی امن مابین یک وب سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعاتی که ما بین وب سرور و مرورگر اینترنت (کاربر) انتقال میابد , محافظت میکند تا در این انتقال به صورت محرمانه و دست نخورده باقی بماند .

SSLیک استاندارد صنعتی است و توسط ملیونها وب سایت در سراسر جهان برای برقراری امنتیت انتقال اطلاعات استفاده می شود برای اینکه یک وب سایت بتواند

ارتباطی امن از نوع SSL را داشته باشد نیاز به یک گواهینامه SSL دارد.زمانیکه شما می خواهید SSL را بر روی سرور خود فعال کنید سؤالات متعددی در مورد هویت سایت شما (مانند آدرس سایت) و همین طور هویت شرکت شما (مانند نام شرکت و محل آن) از شما پرسیده می شود. آنگاه سرور دو کلید رمز را برای شما تولید می کند , یک کلید خصوصی (Private Key) و یک کلید عمومی .(Public Key) کلید خصوصی به این خاطر , این نام را گرفته است , چون بایستی کاملا محرمانه و دور از دسترس دیگران قرارگیرد. اما در مقابل نیازی به حفاظت از کلید عمومی نیست و این کلید در قالب یک فایل درخواست گواهینامه یا Certificate Signing Request که به اختصار آنرا CSR مینامیم قرارداده می شود که حاوی مشخصات سرور و شرکت شما بصورت رمز است. آنگاه شما باسیتی که این کد CSR را برای صادرکننده گواهینامه ارسال کنید. در طول مراحل سفارش یک SSL مرکز صدور گواهینامه درستی اطلاعات وارد شده توسط شما را بررسی و تایید می‌کند و سپس یک گواهینامه SSLبرای شما تولید کرده و ارسال می کند. وب سرور شما گواهینامه SSL صادر شده را با کلید خصوصیتان در سرور و بدور از دسترس سایرین مطابقت می دهد. سرور شما آنگاه امکان برقراری ارتباط امن را با کاربران خود در هر نقطه دارد. نمایش قفل امنیت SSL پیچیده گیهای یک پروتکل SSL برای کاربران شما پوشیده است لیکن مرورگر اینترنت آنها در صورت برقراری ارتباط امن , وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر می شود. و در هنگامی که شما روی قفل کوچک زرد رنگی که در پایین صفحه IE نمایش داده می شود دوبار کلیک می کنید باعث نمایش گواهینامه شما به همراه سایر جزئیات می شود .گواهینامه های SSL تنها برای شرکتها و اشخاص حقیقی معتبر صادر می شوند. به طور مثال یک گواهینامه SSLشامل اطلاعاتی در مورد دامین , شرکت , آدرس , شهر , استان , کشور و تاریخ ابطال گواهینامه و همینطور اطلاعاتی در مورد مرکز صدور گواهینامه که مسؤول صدور گواهینامه می باشد.



۲-۱ InstantSSL چیست؟

InstantSSL یک Web Server Certificate است که اجازه می دهد مشتریان و وب سایتها بتوانند یک تجارت الکترونیک (e-commerce) ایمن با اتصال کد گذار ی شده SSL برقرار کنند. InstantSSL Web Server Certificateها با ۹۸٪ مرورگرها سازگار هستند.

۲-۲ تکنولوژی پیشرفته تایید کردن (authentication)

با فعال کردن آیکون "LOCK" مرورگرتان، QuickSSL به کاربران آنلاین اطمینان می دهد که شماره کارت اعتبار ی و بقیه اطلاعات محرمانه نم ی توانند د یده شوند، دزدیده شوند یا تغییر یابند. بعلت ا ینکه سیستم authentication خودکار ما از پیشرفته ترینها در صنعت می باشد، مشتریان و شرکای تجاری شما می توانند مطمئن باشند که QuickSSL Web Server Certificate ها فقط برا ی گیرندگانی که کاملا تایید شده هستند، صادر می گردد.

۳–۲ دسترسی آنلاین به پروفایل تجاری تان

بعنوان بخشی از مرحله تدارکاتی با QuickSSL، تجارت شما با ChoicePoint ثبت خواهد شد و یک ChicePoint Unique Identifier (CUI) اختصاص داده خواهد شد که معادل عدد DUNS می باشد. CUI یک پروفایل شرکتی برای کاربر اینترنتی شما از طریق اطلاعات موجود در certificate تان، فراهم می کند. اطلاعات پروفا یل تجاری، شامل اطلاعات اولیه گزارش شده از CSR تان از قبیل نام دومین، نام شرکت، بخش، کشور، استان و شهر می باشد. ChoicePoint اجازه می دهد اشخاص معتمد بتوانند اطلاعات بیشتری در مورد شرکت شما را مشاهده کنند و خریداری نمایند . با دسترسی به اطلاعات شرکتی شما، مشتریان تان به برقراری یک تجارت آنلاین اطمینان پیدا خواهند کرد.

۳– مفاهیم رمز گذاری

۳–۱ معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل م ی‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کساری خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روش ی که تام ین کننده ا ین مساله باشد "رمزنگاری" نام دارد. رمزنگار ی هنر نوشتن بصورت رمز است بطوریکه ه یچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخففها و اصطلاحات مخصوص به خود را دارد. برا ی درک عمیق‌تر به مقدار ی از دانش ریاضیات نیاز است. برا ی محافظت از دیتای اصلی (که بعنوان plaintext شناخته می‌شود)، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده (که بعنوان ciphertext شناخته می‌شود) بصورت یک سری بی‌معنی از بیتها بدون داشتن رابطه مشخص ی با د یتای اصلی بنظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آنرا رمزگشایی می‌کند . یک شخص ثالث (مثلا یک هکر) می‌تواند برای اینکه بدون دانستن کلید به د یتای اصلی دست یابد، کشف رمزنوشته (cryptanalysis) کند. بخاطرداشتن وجود این شخص ثالث بسیار مهم است.

<u>رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید.</u>

<u>الگوریتم</u> : یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند.

<u>کلید</u> : یک رشته از ارقام دودویی (صفر و یک) است که بخود ی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پ یاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچ ینی م ی‌شود؛ این عمل عموما بعنوان scrambling شناخته می‌شود. بصورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد . البته دیتای اولیه نمی‌تواند از hashed value بازساز ی شود. Hash functionها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ا ی از پیام (شامل مهم‌ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.

یک چک تا یید پیام (Message Authentication Check) یا MAC یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده م ی‌شود، منجر به ایجاد امضای دیجیتال (digital signature) می‌شود.

۲-۳ الگوریتم‌ها

طراحی الگوریتمهای رمزنگار ی مقوله‌ا ی برا ی متخصصان ر یاضی است. طراحان سیستمهایی که در آنها از رمزنگار ی استفاده م ی‌شود، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصم یم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون (Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پا ی رمزنگار ی به پیش آمده است و الگو ریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابرا ین تعداد الگور یتمهای استفاده شده در س یستمهای کامپیوتری عملی و در سیستمها ی برپایه کارت هوشمند بسیار کم است.

۳-۳ رمزنگاری کلید – عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود . کلید خصوصی صرفا" متعلق به کامپیوتر فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهایی که قصد برقراری ارتباط با یکدیگر را دارند ، گذاشته می شود. برای رمزگشایی یک پیام رمز شده ، کامپیوتر م ی بایست از کلید عمومی که توسط فرستنده ارائه شده، بهمراه کلید خصوص ی خود استفاده نماید. یکی از متداولترین برنامه ها ی رمزنگار ی در این رابطه PGP(Pretty Good Privacy) است . با استفاده از PGP می توان هر چیز دلخواه را رمز نمود.

بمنظور پیاده سازی رمزنگاری کلید - عمومی در مقیاس بالا نظیر یک سرویس دهنده وب ، لازم است از رویکردها ی دیگر ی در این خصوص استفاده گردد. " امضا ی دیجیتال " یکی از رویکردهای موجود در این زمینه است یک امضای دیجیتالی صرفا" شامل اطلاعات محدودی بوده که اعلام می نماید ، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام " امضای مجاز " ، امین اطلاعات است . "امضای مجاز " بعنوان یک میانجی بین دو کامپیوتر ایفای وظیف می نماید. هویت و مجاز بودن هر یک از کامپیوترها برای برقراری ارتباط توسط سرویس دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.

یکی از متداولترین نمونه های پیاده ساز ی شده از رمزنگار ی کلید- عموم ی ، روش SSL(Secure Sokets Layer) است . روش فوق در ابتدا توسط "نت اسکیپ " پیاده سازی گردید. SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب بمنظور ارسال اطلاعات حساس ، ا ستفاده م ی گردد. SSL اخیرا " بعنوان بخش ی از پروتکل TLS(Transport Layer Security) در نظر گرفته شده است .

در مرورگر می توان زمان استفاده از یک پروتکل ایمن نظیز TLS را با استفاده از روش های متعدد اعلام کرد. استفاده از پروتکل "https" درعوض پروتکل "http" یکی از روش های موجود است . در چنین موارد ی در بخش وضعیت پنجره مرورگر یک "Padlock" نشان داده خواهد شد.

رمزنگاری کلید - عموم ی ، مدت زمان زیاد ی را صرف انجام محاسبات م ی نماید. بنابراین در اکثر سیستمها از ترکیب کلید عمومی و متقارن استفاده می گردد. زمانی که دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می نمایند ، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید - عمومی ، ارسال خواهد کرد. در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگار ی کلید متقارن می باشند. پس از اتمام ارتباط ، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد ، می بایست مجددا" فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن ، ....)

۴-۳ مقدار Hash

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدار hash ، استوار است . مقدار فوق ، بر اساس یک مقدار ورودی که دراختیار الگوریتم hashing گذاشته می گردد ، ایجاد می گردد. در حقیقت مقدار hash ، فرم خلاصه شده ای از مقدار اولیه ای خود است . بدون آگاه ی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید بنظر می رسد . مثال زیر نمونه ای در این زمینه را نشان می دهد :

عدد ورودی الگوریتم Hash مقدار

Input # x 143 1,525,381 ۱۰,۶۶۷

تسخیص اینکه عدد ۱.۵۲۵.۳۸۱ (مقدار hash) از ضرب دو عدد ۱۰.۶۶۷ و ۱۴۳ بدست آمده است ، کار بسیار مشکلی است . در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است ، تشخیص عدد دوم کار بسیار ساده ای خواهد بود. (عدد ۱۰.۶۶۷) .رمز نگار ی مبتنی بر کلید عمومی بمراتب پیچیده تر از مثال فوق می باشند. مثال فوق صرفا " ایده اولیه در این خصوص را نشان می دهد.

کلیدهای عمومی عموما" از الگوریتم های پیچیده و مقادیر Hash بسیار بزرگ برا ی رمزنگاری استفاده می نمایند. در چنین مواردی اغلب از اعداد ۴۰ و یا حتی ۱۲۸ بیتی استفاده می شود. یک عدد ۱۲۸ بیتی دارای ۱۲۸ ۲ حالت متفاوت است .

۵-۳ آیا شما معتبر هستید ؟

همانگونه که در ابتدای بخش فوق اشاره گردید ، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر ، در ابتدا رمز و سپس ارسال خواهند شد. کامپیوتر دوم (گیرنده) ، پس از دریافت اطلاعات می بایست ،اقدام به رمزگشایی آنان نماید. یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات توسط یک منبع ایمن و مطمئن ، استفاده از روش معروف " اعتبار سنجی " است . در صورتیکه اطلاعات "معتبر " باشند ، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده اند. با ترکیب فرآیندها ی رمزنگاری و اعتبار سنج ی م ی توان یک محیط ایمن را ایجاد کرد .

بمنظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر رو ی یک کامپیوتر از روش های متعددی استفاده می شود :

- رمز عبور . استفاده از نام و رمز عبور برای کاربران ، متداولترین روش "اعتبار سنجی " است . کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق ، بررسی می گردند. در صورتیکه نام و یا رمز عبور نادرست باشند ، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد.

- کارت های عبور . این نوع کارت ها دارا ی مدل های متفاوتی می باشند. کارت ها ی دارای لایه مغناطیسی (مشابه کارت های اعتباری) و کارت های هوشمند (دارای یک تراشه کامپیوتر است) نمونه هایی از کارت های عبور می باشند.

- امضای دیجیتالی . امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی (نظیر: نامه الکترونیکی ، فایل ها ی متنی و ...) است . استاندارد امضای دیجیتالی (DSS) ، بر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای دیجیتالی (DSA) ایجاد می گردد.الگوریتم فوق شامل یک کلید عمومی (شناخته شده توسط صاحب اولیه سند الکترونیکی - امضاء کننده) و یک کلید عمومی است . کلید عمومی دارای چهار بخش است . در صورتیکه هر چیزی پس

از درج امضای دیجیتالی به یک سند الکترونیکی ، تغییر یابد ، مقادیر مورد نظر ی که بر اساس آنها امضای دیجیتالی با آن مقایسه خواهد شد ، نیز تغییر خواهند کرد.

سیستم های متعددی برای "اعتبار سنجی " تاکنون طراحی و عرضه شده است . اکثر سیستم های فوق از زیست سنجی برای تعیین اعتبار استفاده می نمایند. در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می گردد. برخ ی از روش های اعتبار سنجی مبتنی بر زیست شناسی کاربران ، بشرح زیر می باشند :

- ☑ پیمایش اثر انگشت (انگشت نگاری)
- ☑ پیمایش شبکیه چشم
- ☑ پیمایش صورت
- ☑ مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات ، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است . می بایست این اطمینان بوجود آید که اطلاعات دریافت شده ، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده اند. در این راستا از روش های متعددی استفاده می گردد :

● Checksum . یکی از قدیمی ترین روش های استفاده شده برای اطمینان از صحت ارسال اطلاعات است . Checksum ، به دو صورت متفاوت محاسبه می گردد . فرض کنید Checksum یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد ، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن (صفر و یا یک) را می تواند داشته باشد. در چنین حالتی ۲۵۶ وضعیت متفاوت می تواند وجود داشته باشد. با توجه به اینکه در اولین وضعیت ، تمام هشت بیت مقدار صفر را دارا خواهند بود ، م ی تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی ، ۲۵۵ و یا کمتر باشد ، مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود.

▪ در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی ، بیش از ۲۵۵ باشد ، Checksum معادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵۶ تقسیم نمائیم .

مثال زیر ، عملکرد Checksum را نشان می دهد.

Byte 1 Byte 2 Byte 3 Byte 4 Byte 5 Byte 6 Byte 7 Byte 8 Total Checksum

۱۲۷ ۱,۱۵۱ ۸۰ ۱۷۹ ۱۵ ۲۴۴ ۱۳۵ ۵۴ ۲۳۲ ۲۱۲

(round to 4) ۴.۴۹۶ = ۲۵۶ / ۱,۱۵۱

x 256 = 1,024 ۴

۱۲۷ = ۱,۰۲۴ - ۱,۱۵۱

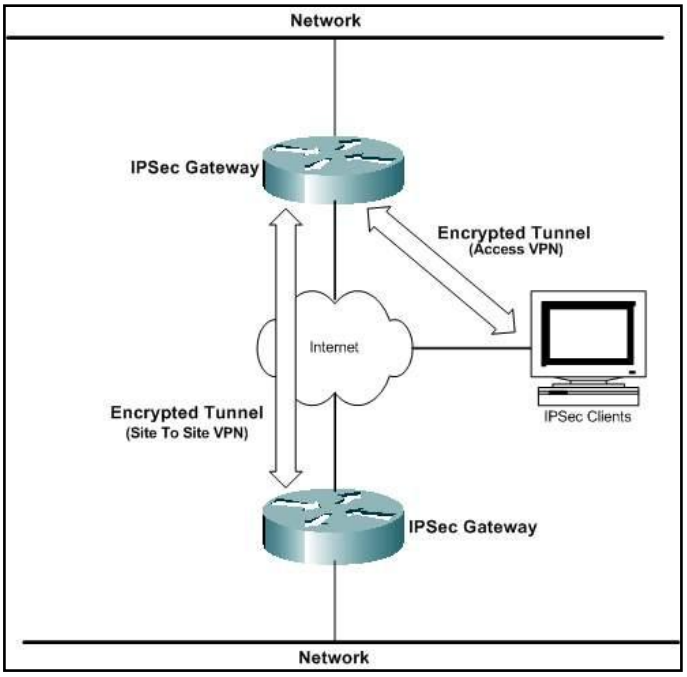
● CRC(Cyclic Redundancy Check) . روش CRC در مفهوم مشابه روش Checksum است . روش فوق از تقسیم چمد جمله ای برای مشخص کردن مقدار CRC استفاده می کند. طول CRC معمولا" ۱۶ و یا ۳۲ بیت است . صحت عملکرد روش فوق بسیار بالا است . در صورتیکه صرفا" یک بیت نادرست باشد ، CRC با مقدار مورد نظر مطابقت نخواهد کرد.

روش های Checksum و CRC امکانات مناسبی برا ی پیشگیر ی از بروز خطا ی تصادفی درارسال اطلاعات می باشند، روش های فوق در رابطه با حفاظت اطلاعات و ایمن سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات ، امکانات محدودتری را ارائه می نمایند. رمزنگاری متقارن و کلید عموم ی ، امکانات بمراتب مناسب تری در این زمینه می باشند.

بمنظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه های اختصاصی ، از روش های متعدد ایمنی استفاده می گردد. ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر : تلفن ، پست ایمن تر می باشد . برای تحقق امرفوق می

بایست از روش های متعدد رمزنگاری و پروتکل های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه های کامپیوتری خصوصا" اینترنت استفاده کرد.

۶-۳ سیستمهای کلید متقارن



یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود دارد data encryption algorithm یا DEA است که بیشتر بعنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوکهای ۶۴بیتی دیتا توسط یک کلید تنها که معمولا ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و براحتی می‌تواند توسط پردازنده‌های کند (بخصوص آنهایی که در کارتهای هوشمند وجود دارند) انجام گیرد.

این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلا هویت یکدیگر را تایید کرده‌اند عمر کلیدها بیشتر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES۴۰بیتی امروزه در عرض چند ین ساعت توسط کامپیوترهای معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی

اعتبار استفاده شود. کلید ۵۶بیتی عموما توسط سخت‌افزار یا شبکه‌ها ی بخصوص‌ی شکسته می‌شوند. رمزنگاری DESسه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر)
این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواه یم دید که ا ین یک عامل مهم در قدرت رمزکنندگی است.

الگوریتمهای استاندارد جد یدتر مختلف‌ی پیشنهاد شده‌اند. الگور یتمهایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما ه یچکدام پیاده‌سازی سخت‌افزاری نشدند بنابراین بعنوان رقیبی برای DES برا ی استفاده در کاربردها ی میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جایگزیتی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصا برا ی پیاده‌سازی در پردازنده‌ها ی توان-پایین مثلا در کارتهای هوشمند طراحی شد.

در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمها Skipjack و مبادله کلید را که در کارتهای Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیشتر کارتهای هوشمند برپایه این الگور یتم ها بود.

برای رمزنگاری جریانی (streaming encryption) (که رمزنگار ی دیتا در ح ین ارسال صورت می‌گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC4 سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم م ی‌کند . RC4 که متعلق به امنیت دیتای RSA است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

۷-۳ سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برا ی رمزنگار ی و رمزگشا یی استفاده می‌کنند. بسیاری از سیستمها اجازه می‌دهند که یک جزء (کلید عموم ی یا public key) منتشر شود در حالیکه دیگری (کلید اختصاصی یا private key) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند . بعبارتی تنها با کل ید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای بجز گ‌یرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمولتر ین سیستم نامتقارن بعنوان RSA شناخته م ی‌شود (حروف اول پدیدآورندگان آن یعنی Rivest، Shamir و Adlemen است). اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشاندادن ا ینکه فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحا امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توانهای خیلی طولانی دارد:

امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛

رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر ا ینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشا یی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به ا ین ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمزشده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Yk \pmod r$

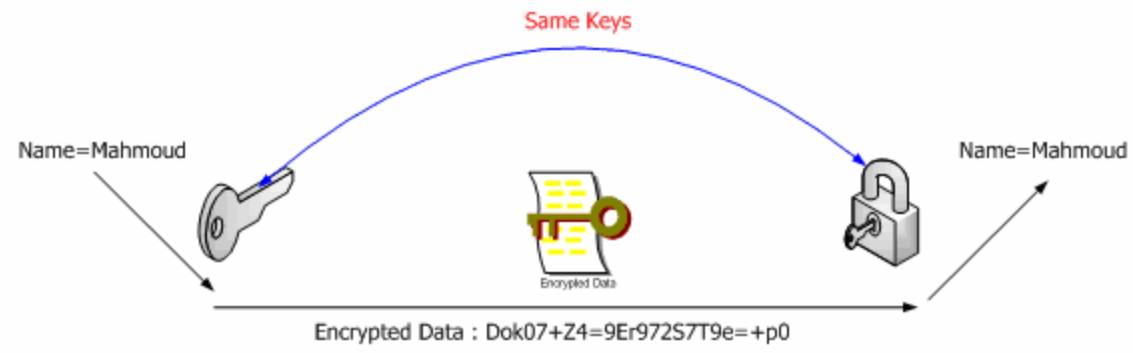
که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصلضرب دو عدد اول یه بزرگ است که با دقت انتخاب شده‌اند. برای اطلاع از جزییات بیشتر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد. این شکل محاسبات روی پردازنده‌ها ی با یتی بخصوص روی ۸ بیتی‌ها که در کارتهای هوشمند استفاده می‌شود بس‌یار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن م ی‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده م ی‌شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگار ی کلیدهای آتی استفاده می‌شود.

سایر سیستمهای کلید نامتقارن شامل سیستمهای لگار یتم گسسته م ی‌شوند مانند Diffie-Hellman، ElGamal و سایر طرحهای چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرحها عملکردهای یک‌ـطرفه‌ای دارند که اجازه تاییدهویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده م ی‌کند . RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگار ی و رمزگشا یی (برا ی یک طرح کلید عمومی) رشته‌هایی از دیتا بطور استثنایی کاراست و می‌تواند براحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین بخوبی با رمزنگار ی و تصد یق‌هویت در ارتباطات سازگار است.

طولهای کلیدها برای این طرحهای جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در RSA است که آنها برای استفاده در چیپ‌کارتها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از ا ین الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می‌رود.

اساس رمز گذاری ها وجود کلید ها می باشند.بدین معنی که شما اطلاعات مورد نظر خود را توسط کلید قفل می کنید و سپس برای رمزگشایی آن مجددا از کلید استفاده می کنید .در رمز گشایی با کلید متقارن ، هر دو کلیدی که برای قفل و باز کردن

اطلاعات استفاده می شود یکسان می باشد .بدین معنی که هر دو طرف از یک کلید یکسان بهره می برند که باید نزد خودشان امن باشد.
توجه کنید که مفهوم کلید در مباحث مرتبط ، عموما یک آرایه از بایت ها می باشد که بر اساس نوع امنیت طول متفاوتی دارد.مثلا ۰۱۱۰۱۱۰۰۱۱۰۰۱۰۱۱۱۰۰۱ می تواند یک کلید باشد.البته عموما کلید ها در مبنای ۱۶ نمایش داده می شوند .به هر حال وظیفه محافظت از کلید بر عهده دارنده آن است!
در شکل زیر نحوه رمز گذاری اطلاعات توسط کلید متقارن نمایش داده شده است:

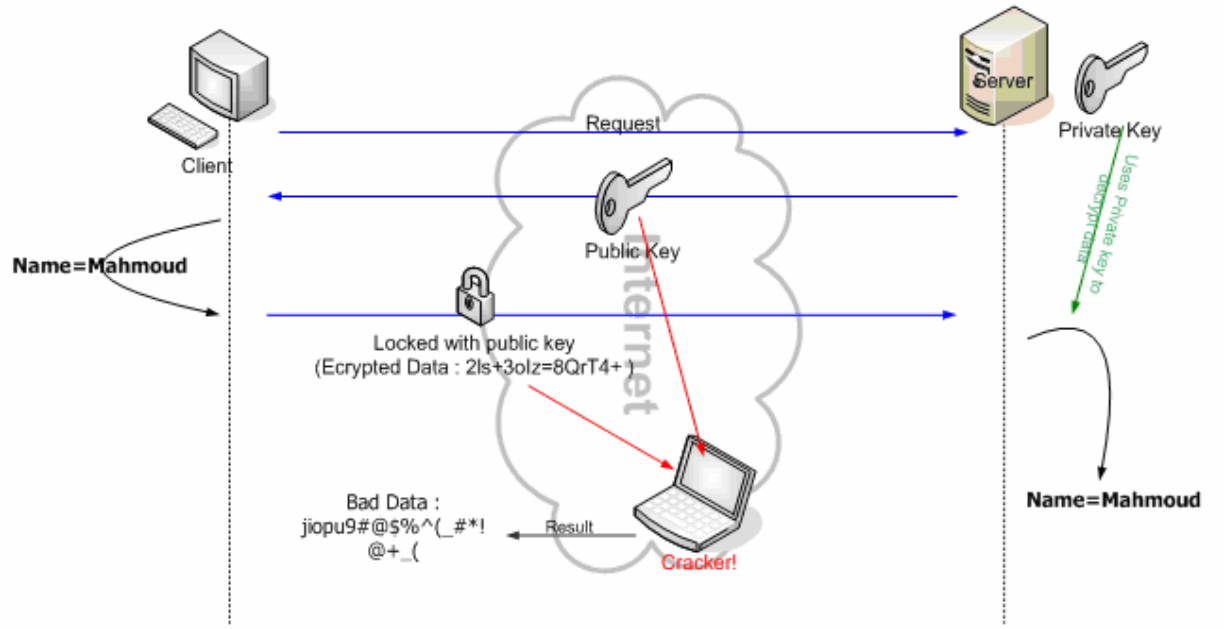


گذاری که رمز گذاری نا متقارن یا رمز گذاری کلید عمومی نامیده می شود ، دو نوع کلید وجود دارد:
کلید عمومی
در این رمز گذاری گفته می شود که اگر داده ای با یک کلید قفل شد ، با همان کلید باز نمی شود و فقط امکان باز شدن

آن با کلید متناظر آن وجود دارد .این کلید متناظر نزد طرف مقابل است و امکان بدست آوردن آن از کلید دیگر وجود ندارد .به عبارت ساده تر اگر شما در خانه تان را با کلید A قفل نمودید ، تنها امکان باز شدن آن با کلید متناظرB وجود دارد و این در حالیست که امکان فهمیدن آنکه کلید B چگونه ساخته شده است برای شما نیز وجود ندارد. حال اگر کلید خود را درون در نیز جا بگذارید ، مساله ای نیست!

حال به بحث باز می گردیم : شما درخواست داده ای را از یک سرور امن می کنید ، سرور کلید عمومی را برای شما ارسال می کند . شما داده های خود را با این کلید

قفل می کنید و برای سرور ارسال می کنید .حال اگر این وسط کسی خواست داده ها را ببیند ، نمی تواند ، چراکه این داده ها با کلید عمومی باز نمی شوند .!در طرف مقابل سرور با کلید خصوص خود داده ها را رمز گشایی می کند و از آن استفاده می کند.
شکل زیر روند ذکر شده را می رساند:



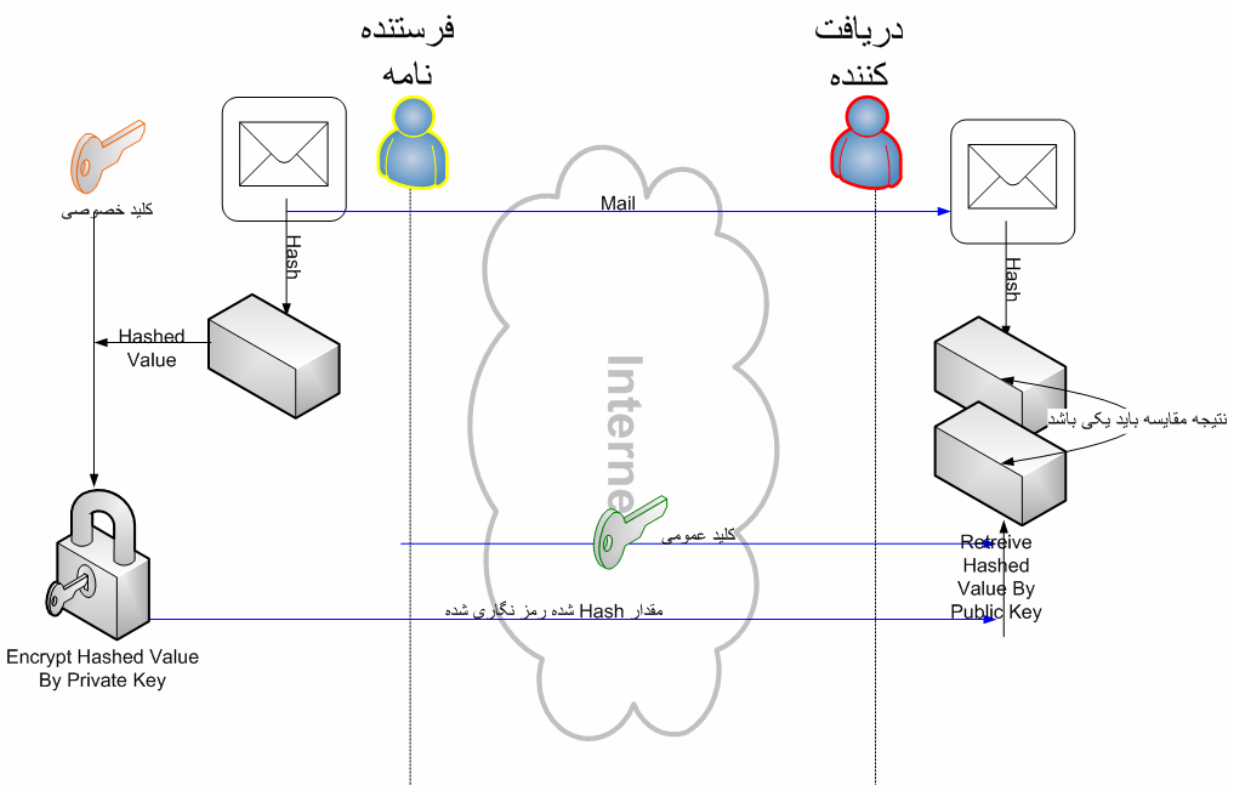
توجه : در امضای دیجیتالی روند برعکس است).به عبارت دیگر امضای دیجیتالی چیزی جز رمز گذاری داده ها با کلید خصوصی فرستنده نیست .(ما در امضای دیجیتالی می خواهیم ببینیم که آیا داده های ارسال شده واقعاً از طرف شخصی است که ادعا می کند یا خیر؟
به طور ساده کاربر نام خود را با کلید خصوصی خود رمز گذاری می کند .در این حالت همه با کلید عمومی وی می توانند نام وی را رمز گشایی کنند و این صحیح است ! چراکه هیچ کس دیگر قادر نیست داده ای تولید کند که نتیجه باز شدن آن با کلید عمومی شخص امضا کننده برابر باشد.!
البته در عمل بهتر است از توابع Hash استفاده می شود .چراکه در حالت فوق ، اولا نام کاربر را باید فقط کاربر و سرور بدانند و دیگر آنکه از کجا معلوم که داده ارسالی همانی است که امضای دیجیتالی کاربر با آن بوده است (به عبارت دیگر شاید در میان راه متن اطلاعات تغییر کرد)

همانطور که ذکر شد ، در این مورد از توابع Hash که یک طرفه هستند استفاده می شود.بدین معنی که اگر داده ای hash شد ، دیگر به هیچ عنوان) و توسط هیچ کلیدی (قابل برگشت نیست.

بدین منظور متن نامه ابتد hash می گردد و سپس توسط کلید خصوصی امضا می شود.

سپس امضا و متن نامه ارسال می شود .در طرف سرور هم با کلید عمومی داده hash شده بدست می آید .متن ارسالی همhash می شود. حال اگر این دو نتیجه یکسان بود ، داده ها واقعًا از طرف کسی که مدعی آن است ارسال شده است .چرا که اگر متن نامه عوض شود ، نتیجه hash آن هم متفاوت و مقایسه نتیجه یکسانی را بر نمی گرداند.

در نمودار زیر ، روند کار را مشاهده می کنید (قطعه های خاکستری رنگ نشان دهنده Hash شدن متن نامه می باشند)



۴- ساختار و روند آغازین پایه گذاری یک ارتباط امن

در این پروتکل قبل از آنکه اطلاعاتی مابین درخواست دهنده و سرور رد و بدل شود ، می بایست ابتدا سرور تصدیق گردد .[۲]

به طور کلی مرحله آغازین شروع ایجاد ارتباط امن[۳] از دو فاز تشکیل شده است : تصدیق هویت سرور و مرحله اختیاری تصدیق هویت مشتری .در فاز تصدیق هویت سرور ، سرور در جواب درخواست مشتری گواهینامه خود و فرمول رمز گذاری خود[۴] را برای مشتری ارسال می کند .سپس مشتری یک کلید اصلی [۵]که با کلید عمومی[۶]سرور رمز گذاری شده است را تولید میکند و سپس این کلید رمز گذاری شده را به سرور ارسال می کند .سرور کلید اصلی را بازیابی می کند و خودش را با فرستادن پیغامی به مشتری تصدیق می نماید .درخواست های بعدی با کلید هایی که از کلید اصلی مشتق شده اند رمز گذاری و تصدیق می شوند. در فاز دوم که اختیاری بود ، سرور یک چالش[۷] را برای مشتری ایجاد می کند ارسال می کند .مشتری نیز خودش را برای سرور با ارسال امضای دیجیتالی و گواهینامه کلید عمومی خود[۸]نسبت به تصدیق خود اقدام می نماید.

الگوریتم های زیادی جهت پنهان سازی درSSL استفاده می شوند .در مرحله آغازین شروع ایجاد ارتباط امن از الگوریتم RSA public-key cryptosystem استفاده می شود .بعد از رد و بدل شدن کلید ها نیز الگوریتم های متفاوتی استفاده می شوند . از جمله : RC ۲ ، RC۴ ، IDEA ، DES ، triple-DES و MD۵ .

گواهینامه های کلید عمومی هم از قوانین X.۵۰۹ پیروی می کنند (ساختار درختی CA ها و امضای گواهینامه ها که در ادامه ذکر خواهد شد ، همگی بر اساس این استاندارد است)

۴-۱ پروتکل های مشابه

[۹] TLS هم پروتکل ای است که بسیار مشابه SSL ۳,۰ می باشد.

همچنین پروتکل [۱۰] WTLS که مخصوص شبکه های بیسیم است و در WAP استفاده می گردد[۱۱].

۵- مفهوم گواهینامه در پروتکلSSL

در اینجا نیاز است که یک بحث کلی در مورد گواهینامه[۱۲] مورد نیاز این پروتکل صورت گیرد.به طور عموم (غیر از بحث SSL) گواهینامه ها جنبه اعتبار سنجی دارند . بدین معنی که اگر شما در یک بحث خاص دارای گواهینامه باشید ، به شما اعتماد بیشتری می کنند.اما ممکن است گواهینامه نداشته باشید ولی کار خود را هم به نحو احسنت انجام دهید.به طور مثال شما قهرمان مسابقات فرمول ۱ جهان هستید ، اما در صورتی که گواهینامه نداشته باشید ، هرگز اجازه نخواهید داشت که در شهر تردد کنید!

در مورد SSL هم تقریبا بحث به همین گونه است با این تفاوت که ذات این پروتکل با توجه به بحث گواهینامه ها طراحی شده است بدین معنی که اگر دارای گواهینامه نباشید ، قادر نخواهید بود که یک پیاده سازی از این پروتکل را داشته باشید.شاید در عالم راندن اتومبیل بدین صورت تعبیر شود که در صورتی که شما دارای گواهینامه نباشید ، قادر به رانندگی هم نیستید ! این تشابه از جهاتی صحیح و از جهاتی غلط است . شاید برداشت صحیح تر به این صورت باشد که اگرچه قادر نخواهید بود بدون گواهینامه رانندگی کنید ، اما قادر هستید که خود برای خود یک گواهینامه صادر کرده و سپس به رانندگی بپردازید)!هرچند این گواهینامه از نظر دیگران کاملا بی ارزش است!) .

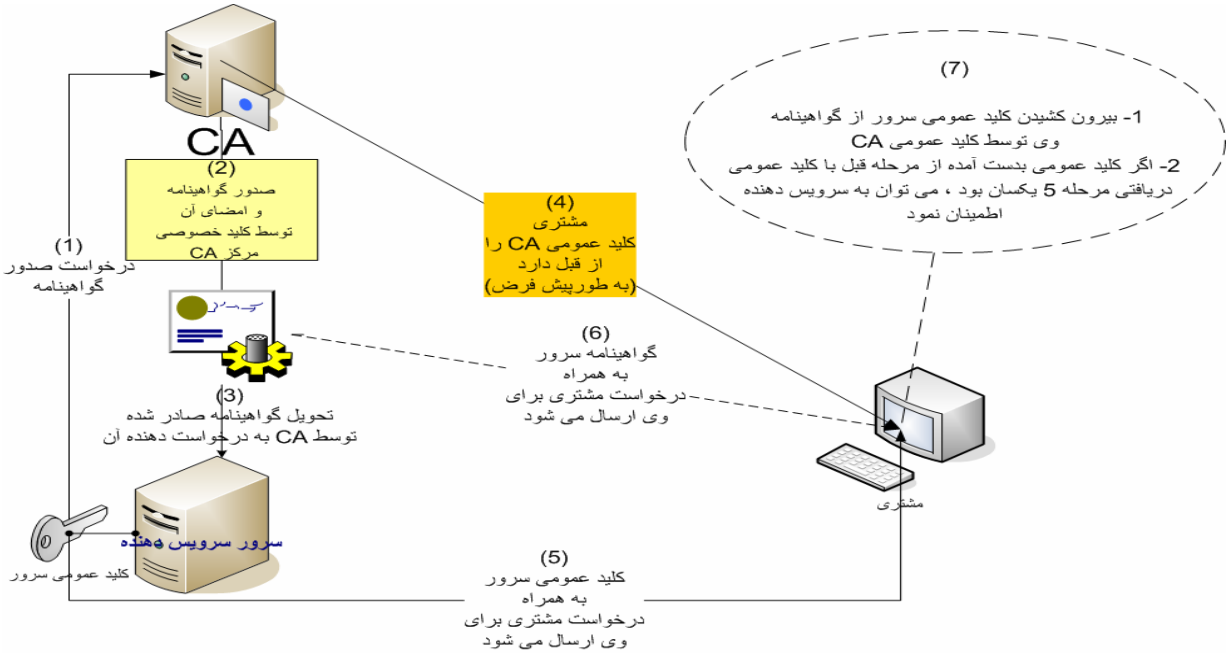
طبق بحث فوق ، شما قادر خواهید بود بدون پرداخت هیچ هزینه ای یک پروتکل SSL را راه اندازی و استفاده نمایید.نمونه بارز این استفاده در شبکه های داخلی یا Intranet می باشد.

۵-۱ مراکز صدور گواهینامه

در SSL به مراکزی که اقدام به صدور گواهینامه می کنند ،" مرکز صدور گواهینامه " [۱۳]یا به اختصارCA گفته می شود.

این پروتکل از یک شخص ثالث [۱۴] (که همان CA می باشد) برای تشخیص هویت طرفین یک تراکنش استفاده می کند . در واقع یک گواهینامه معین می کند که آیا شخصی که دارنده آن است ، واقعًا همانی است که ادعا می کند یا خیر؟

در شکل زیر می توانید یک روند درخواست صدور گواهینامه توسط یک سرویس دهنده (قدم های ۱، ۲و۳) و در ادامه آن درخواست کاربر برای یک سرور دارای گواهینامه و چگونگی مطمئن شدن وی از معتبر بودن آن سرور را ببینید (قدم های ۶،۵،۴و۷) :



۲–۵ مراحل کلی برقراری و ایجاد ارتباط امن در وب

به طور ساده مراحلی که در ایجاد یک ارتباط امن SSL در http طی می شود ، به صورت زیر می باشد:

۱ - کاربر درخواست خود را از طریق مرورگر به یک صفحه امن ارسال می کند (آدرس این صفحه معمولا با // : https شروع می شود)

۲ - وب سرور کلید عمومی خود را به همراه گواهینامه خود برای کاربر ارسال می کند.

۳ - مرورگر چک می کند که آیا این گواهینامه توسط یک مرکز مورد اطمینان صادر شده است و اینکه آیا این گواهینامه هنوز اعتبار دارد ؟ و همچنین آیا این گواهینامه مرتبط با سایت درخواستی می باشد؟

۴ - سپس مرورگر از این کلید عمومی دریافت شده از طرف سرور استفاده می کند سپس یک کلید متقارن را رمز گذاری می کند .در نهایت هم داده های رمز URL تصادفی را تولید می کند و توسط آن تمام داده ها و گذاری شده را به همراه خود کلید متقارن تولیدی ، مجددا توسط کلید عمومی سرور رمز گذاری کرده و نتیجه را به سرور ارسال می کند.

۵ - وب سرور توسط کلید خصوصی خود، کلید متقارن رمز گذاری شده را رمزگشایی و با استفاده از آن سایر داده ها وURL را نیز رمزگشایی می نماید.

۶ - وب سرور ، html درخواستی را با کمک کلید متقارن رمز گذاری و به کاربر باز می گرداند.

۷ - مرورگر نیز داده های دریافتی را با کمک کلید متقارن خود بازگشایی کرده و به کاربر نمایش می دهد.

همانطور که از مرحله ۳ پیداست ، در این مرحله است که میزان اعتبار CA مشخص می شود .در صورتی که اینCA به هر دلیل از نظر مرورگر دارای اعتبار و شرایط خاصی نباشند ، هشداری مبنی بر عدم امن بودن سایت مورد نظر به کاربر ارایه می دهد . توجه کنید که در این مورد تنها به هشدار بسنده می شود ، اطمینان به آن به شما و شرایط شما بستگی دارد . در ضمن آنکه این هشدار هرگز نمی تواند به معنای قطعی عدم وجود امنیت باشد.حال اگر شما یک CA اینترنت راه اندازی کردید ، مسلما هیچ کدام از مرورگر ها شما را نمی شناسند و بنابراین گواهی های صادر شده از طرف شما را نا امن می پندارند.از آنجا که کاربران عادی اینترنت نیز این هشدار ها را جدی در نظر می گیرند ، از ادامه تراکنش با سایت شما صرف نظر خواهند کرد.

۳–۵ نکاتی در مورد گواهینامه ها

شما در صورتی به یک سایت با یک گواهینامه معین اعتماد می کنید که آنرا یک CA معتبر (حداقل نزد شما) امضا کرده باشد.در واقع این اعتماد شما ضمنی است .به این روند ، درخت اعتبار گواهینامه یا مسیر گواهینامه گفته می شود .

- معمولا مرورگرها تعدادی از CA ها ی معروف را برای خود در نظر می گیرد.
- CA های متفاوتی در اینترنت وجود دارد که شاید مشهورترین verisign آن باشد.به هر حال قرار نیست شما همیشه ، با توجه به تراکنش خود، به تمام

CA ها)یا به عبارت بهتر به انواع گواهینامه آنها (اعتماد کنید .یک راه مناسب برای تشخیص این موضوع میزان مبلغی است که گواهینامه مورد نظر تراکنش شما را بیمه می کند.به طور مثال حداکثر مبلغی که iranSSL تراکنش شما را بیمه می کند ۱۰،۰۰۰ دلار می باشد .اما Verisign گواهینامه ای دارد که تا ۲۵۰,۰۰۰ دلار تراکنش شما را بیمه می نماید .(بسیار مشابه با وضعیت شرکت های بیمه)

- پروتکلSSL بر اساس میزان امن بودن دسته بندی می شوند .این دسته بندی بر اساس مقدارbit های تولیدی به ازاء هر بخش از داده ای است که رمز گذاری می شود.مسلما هرچه تعداد این bit های تولیدی بیشتر باشد ، رمزگشایی آن بدون کلید ، بسیار سخت تر و با استفاده از کلید نیز زمان برتر خواهد بود . به عنوان نمونه یک SSL با ۴۰ یا ۵۶ بیت) که یک رمز گذاری ضعیف می باشد (می تواند توسط یک هکر با ابزار کافی ، در عرض چند دقیقه شکسته شود .اما همین هکر برای مقابله با SSL ۱۲۸ بیتی ، نیاز به ۸۸ ۲ بار زمان بیشتر دارد !و این بدین معنی است که SSL ۱۲۸ بیتی نسبت به حالت ۴۰ یا ۵۶ بیتی ترلیون ترلیون بار امن تر و غیر قابل نفوذ تر است!

یک بحث دیگر اینجا مطرح می شود و آن اینکه اگر یک هکر در میان راه کلید عمومی خود را جایگزین کلید عمومی سرور کرد .در این حالت عملا هکر به راحتی به اطلاعات کاربر دسترسی خواهد داشت . در واقع اینCA ها کلید عمومی سرور را با کلید خصوصی خود امضا می کنند.مرورگر هم CA های قابل اعتماد را می شناسد (کلید عمومی آنها را دارد) . این کلید عمومی سرور که توسط کلید خصوصی CA رمز گذاری شده است همان گواهینامه می باشد.از آنجا که سرور می بایست گواهینامه خود را ارسال کند ، در سمت مرورگر سعی می شود که توسط کلید های عمومی CA هایی را که می شناسد ، آن گواهینامه را رمز گشایی کند.اگر موفق شد و نتیجه با کلید عمومی سرور یکسان بود در واقع گواهینامه قابل اعتماد است.در این صورت امکان استفاده از گواهینامه دیگران هم وجود ندارد).دقیقا همان بحث امضای دیجیتالی است.

۴–۵ تشخیص هویت :

یکی از مباحث مهم و اصول در ارتباطات ایمن ، تشخیص هویت متقابل از هر دو طرف Client و Server می باشد . در یک ارتباط ، می باشد هویت اصلی سرور برای کاربران و برعکس مشخص شود زیرا در غیر این صورت هر سروری قادر به ایجاد اعتماد در کاربران خواهد بود . هر سرور باید دارای گواهینامه دیجیتالی باشد که این گواهینامه ، نشاندهنده هویت اصلی آن است و توسط شرکتهایی مانند Verisign و Thawte ارائه می گردد . در این گواهینامه الکترونیکی اطلاعاتی از قبیل : کلید عمومی (برای مخفی سازی اطلاعات) ، شماره سریال ، نام دامنه ، امضای دیجیتالی و تاریخ شروع و انقضای اعتبار گواهینامه درج می شود .

کاربر به راحتی می تواند مشخصات گواهینامه سرور را بررسی نماید . به عنوان مثال فرض کنید که برای خرید یک کالا به صورت On-lin به یکی از سایتهای مربوطه متصل شده اید ، در ابتدا پیغامی مبنی بر ایجاد یک ارتباط با استفاده از SSL را ملاحظه می کنید ، که بعد از تأیید آن ، اگر به پایین پنجره مرورگر خود از سمت راست (Staus Bar) دقت نمایید ، آیکونی (به شکل یک قفل) را مبنی بر یک ارتباط ایمن مشاهده خواهید کرد که با دوبار کلیک کردن بر روی آن می توانید اطلاعاتی گواهینامه سرور را بطور کامل مشاهده نمایید. البته باید توجه داشته باشید که حتماً مرور گر وب شما قابلیت پشتیبانی از SSL را داشته باشد و یا آن را غیر فعال نکرده باشید . برای اطمینان از فعال بودن این پروتوکل ، در Internet Explorer از منوهای بالا به منوی Tools > Internet Options رفته و از پنجره ظاهر شده ، Tab مربوط به Advanced را انتخاب کرده و از انتخاب گزینه ای با عنوان ۰، ۳ Use SSL اطمینان حاصل کنید . پیشنهاد می کنم که حتماً قبل از استفاده از Credit Card خود در اینترنت ، گواهینامه سرور را از نظر تاریخ انقضا و نام دامنه مورد بررسی قرار دهید .

سرویس‌های امنیتی WEP - Authentication

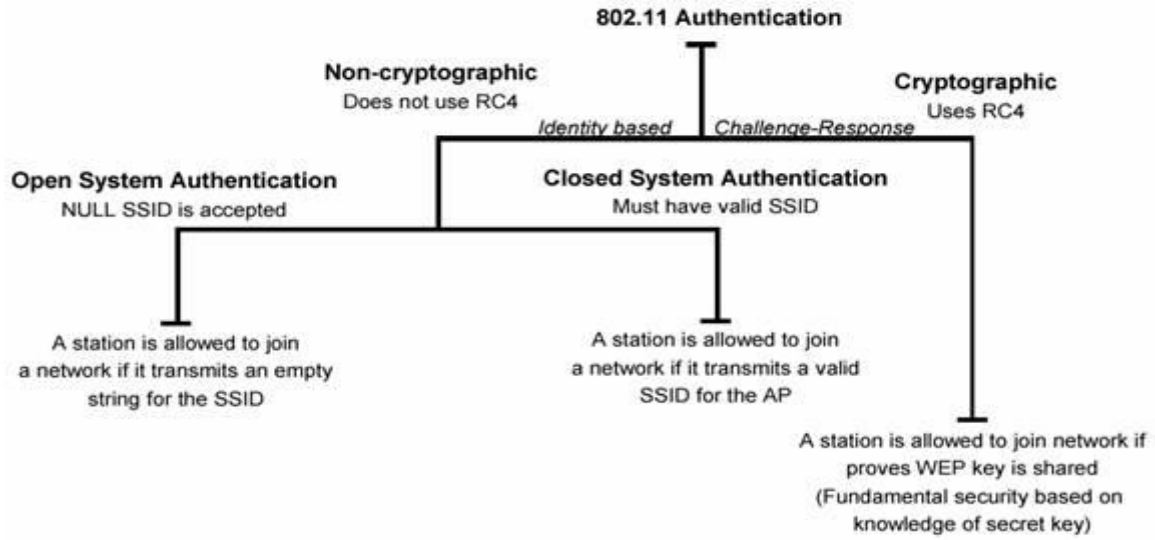
در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد ۸۰۲.۱۱ است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم.

در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

Authentication

استاندارد ۸۰۲.۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد :



همان‌گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می‌کند و روش دیگر از هیچ تکنیک رمزنگاری‌یی استفاده نمی‌کند.

Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدومِ متقاضی پیوستن به شبکه، درخواست ارسال هویت

از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.

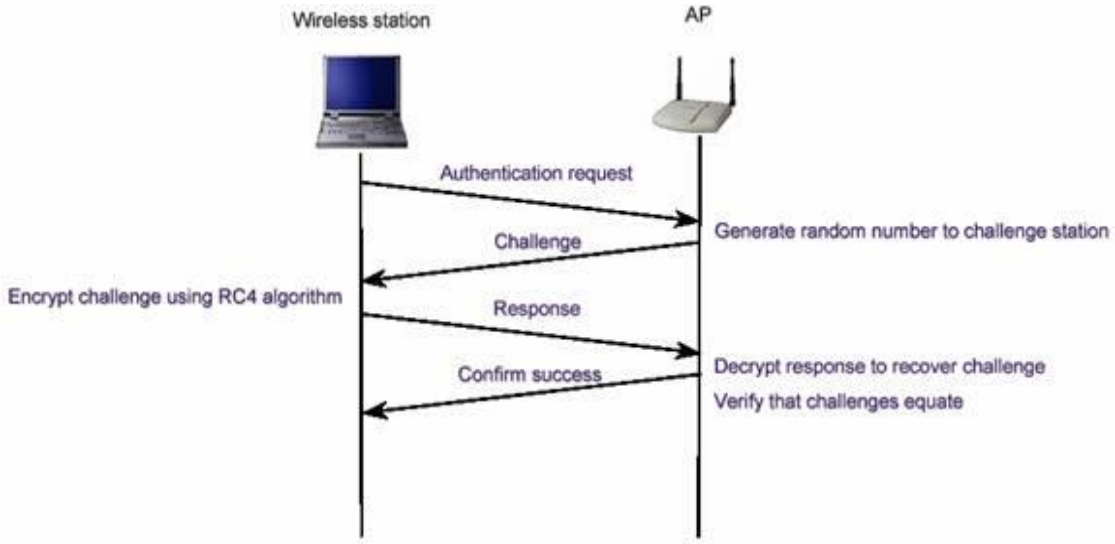
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی‌دهند و عملاً تنها راه‌ی برای آگاه‌ی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ‌دادن حملات نیز خود تضمینی ندارد!

Authentication با رمزنگاری RC4

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد :



در این روش، نقطه‌ی دسترسی (AP) یک رشته ی تصادفی تولید کرده و آن‌را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت همسانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند . روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است :

الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هریک از دو طرف را گمراه می‌کند.

سرویس‌های امنیتی Privacy – 802.11b و Integrity

در قسمت قبل به سرویس اول از سرویس‌های امنیتی 802.11b پرداختیم. این قسمت به بررسی دو سرویس دیگر اختصاص دارد. سرویس اول Privacy (محرمانه‌گی) و سرویس دوم Integrity است.

Privacy

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه‌داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی‌که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

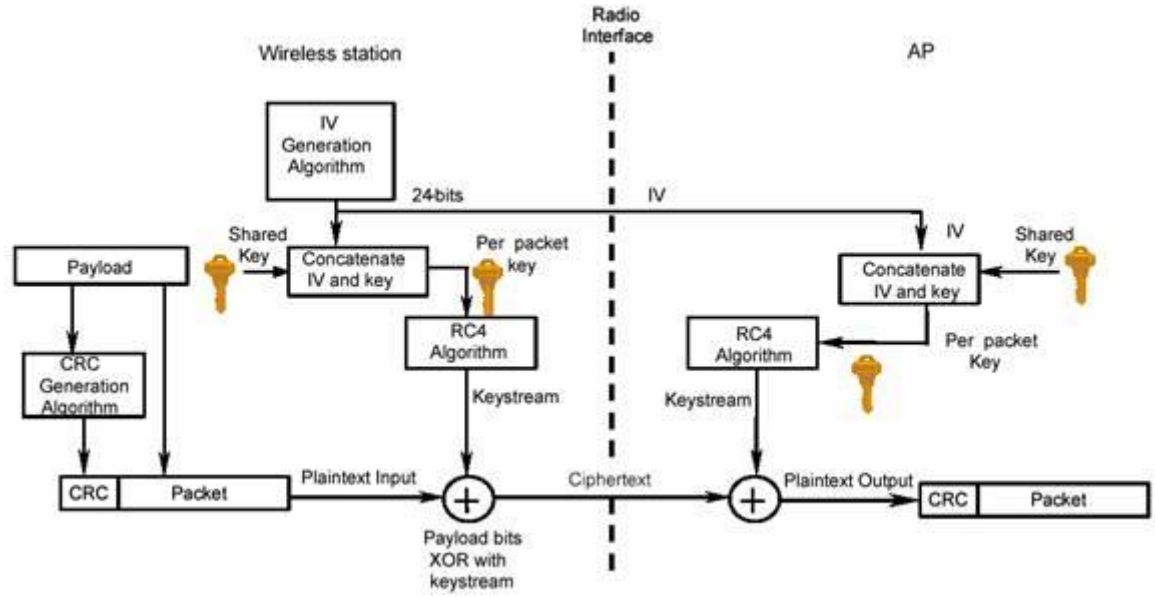
در استاندارد 802.11b، از تکنیک‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود . این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به‌بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه‌های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV(مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که

تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این‌ست که روش تأمین محرمانه‌گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است :



Integrity

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.

در استاندارد 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دست‌رسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به‌صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخ‌داد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمنِ ذکر هریک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌یی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند .

نکته‌یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دست‌یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی‌های بسیاری را برای تعیین حفره‌های امنیتی این استاندارد انجام داده‌اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی‌های انجام شده فهرستی از ضعف‌های اولیه‌ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دست‌رس نفوذگر باشد، کلید آن به‌راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال‌های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

از آن‌جایی‌که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمزشده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن‌جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

۴. استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دست‌رسی بی‌سیم به‌سوی گیرنده ارسال می‌شود بر اساس یک CRC رمزنشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دست‌رسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی

یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به‌راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دست‌رسی بماند که آیا بسته‌ی تأیید را صادر می کند یا خیر.

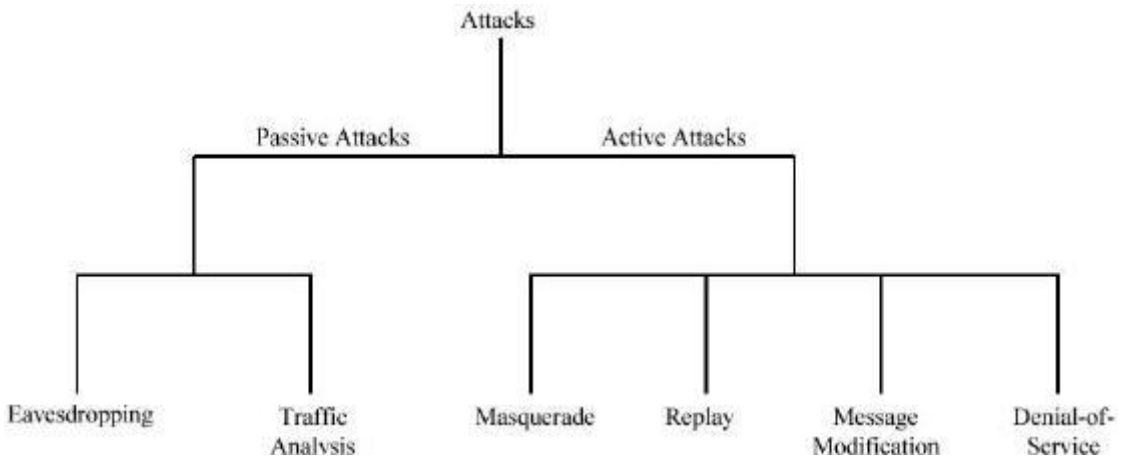
ضعف‌های بیان شده از مهم‌ترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌یی که در مورد ضعف‌های فوق باید به آن اشاره کرد این است که در میان این ضعف‌ها تنها یکی از آن‌ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می‌گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می‌گردد و بقیه‌ی مشکلات امنیتی کماکان به قوت خود باقی هستند.
جدول زیر ضعف‌های امنیتی پروتکل WEP را به‌اختصار جمع‌بندی کرده است :

Security Issue / Vulnerability	Remarks
1. **Security features in vendor products are frequently not enabled.**	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. **IVs are short (or static).**	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. **Cryptographic keys are short.**	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. **Cryptographic keys are shared.**	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. **Cryptographic keys cannot be updated automatically and frequently.**	Cryptographic keys should be changed often to prevent brute-force attacks.
6. **RC4 has a weak key schedule and is inappropriately used in WEP.**	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. **Packet integrity is poor.**	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. **No user authentication occurs.**	Only the device is authenticated. A device that is stolen can access the network.
9. **Authentication is not enabled; only simple SSID identification occurs.**	Identity-based systems are highly vulnerable particularly in a wireless system.
10. **Device authentication is simple shared-key challenge-response.**	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

خطرها، حملات و ملزومات امنیتی

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد :



مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.

حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

- شنود

در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال

شنودترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.

- آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند :

- تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.

- پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه –به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار

گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت وآمد می کنند و هریک از این ترافیک ها و پروتکل ها از شیوه یی برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند. با توجه‌به گسترده گی این نوع حمله، که کاملاً به نوع پروتکل بسته گی دارد، در این جا نمی توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دست رسی – که می تواند یک کاربر عادی باشد – فراهم کند.

- حمله های DoS - Denial-of-Service

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کارانداختن خادم های نرم افزاری و سخت افزاری ست. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه یی ست که مشکلاتی برای نفوذگر برای دست رسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می کند. در برخی از حالات، در پی حمله ی انجام شده، سرویس مورد نظر به طور کامل قطع نمی گردد و تنها کارایی آن مختل می گردد. در این حالت نفوذگر می تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق/به همان سرویس نیز اقدام کند.

تمامی ریسک هایی که در شبکه های محلی، خصوصاً انواع بی سیم، وجود دارد ناشی از یکی از خطرات فوق است .

۶ – مشکلات و معایب SSL

۶–۱ مشکل امنیتی در SSL :

با وجود اینکه این پروتکل امروزه در سایتهای تجارت الکترونیکی مورد استفاده گسترده قرار می گیرد ولی نمی توان منکر معایب و نواقص آن شد . همانطور که می دانید کلید اصلی مربوط به ارتباطات SSL بصورت تصادفی ایجاد می شود ، متأسفانه طاراحی سیستم ایجاد کنند کلید جلسه (Session Key) این پروتوکل که توسط شرکت Netscape ایجاد شده ، ضعیف می باشد ، و یک هکر ماهر به راحتی قادر به پیدا کردن این کلید خواهد بود . نسخه های قبلی SSL از کلید های ۴۰ بیتی استفاده می کردند و نسخه ۳ این پروتوکل از کلید ۱۲۸ بیتی استفاده می کند ، لازم به ذکر است که تمامی نسخه ها این پروتوکل به غیر نسخه ۳ ، توسط مهاجمان ، Crack شده و نا امن است ، البته هنوز نسخه ۳ کرک نشده ، ولی کارشنا سان احتمال وقوع این امر را در آینده ای نزدیک می دهند که در این صورت می بایست تحولات بنیادی در زیر بنای این پروتکل ایجاد شود .

۶–۲ مشکلات تجارت الکترونیکی در ایران :

اولین نکته هیچگاه به همه سایتها اعتماد نکنید و شماره اعتباری خود را در اختیارشان قرار ندهید . بعضی سایتها به بهانه Adult Check و بهانه هایی از قبیل ، شماره کارت اعتباری شما را گرفته و از آن سوء استفاده میکنند . حتی بعضی سایتها گواهینامه های دیجیتالی صحیح و تثبیت شده ای به شما نشان می دهند ولی امکان بروز مشکل همچنان وجود دارد . همیشه از سایتهای معتبر که سیستم های تست شده ای را ارائه می دهند و مورد استفاده عموم قرار گرفته اند استفاده کنید . در این بین ، امکان کلاهبرداری از کاربران ایرانی در اینترنت چند برابر می باشد . زیرا قوانینی برای حمایت از کشورهایی که در اقتصاد جهانی دارای محدودیت هستند وجود ندارد و نظارتی به روی این معاملات انجام نمی گیرد . همچنین خیلی از اجناس خریداری شده به ایران ارسال نمی گردد ، ولی در کشورهای خارجی در صورتی که کالایی بعد از خرید Online به مقصد نرسد بلافاصله توسط مراجع قانونی مورد پیگیری بین المللی قرار خواهد گرفت . یکی از مشکلات مهم دیگر عدم دسترسی به کارتهای اعتباری بین المللی است ، اگر چه گامهای موثر و مثبتی در جهت رفع این مشکل توسط سازمانهای خصوصی و واسطه ای انجام گرفته و حتی در بعضی معاملات از کارتهای اعتباری

داخلی استفاده می شود ولی تجارت الکترونیکی در ایران نیازمند حمایت بیشتری از طرف مسئولین امر می باشد .

ضمیمه ۱ : پیاده سازی SSL در Windows 2000 Server

(با استفاده از وب سرور IIS)

برای اینکه یک سیستم کامل امنیتی با SSL را روی ویندوز سرور ۲۰۰۳ راه اندازی کنیم باید فرآیندهای زیر را طی کنیم:

۱.ایجاد یک وب سایت

۲.اعمال تغییرات بر روی DNS برای ارتباط با IIS

۳.نصب Certificate Service و ایجاد یک Certificate Authority (CA)

۴.ایجاد یک request از طرف وب سرور، برای دریافت Certificate از CA

ایجاد یک وب سایت در IIS

نکته : قبل از این مرحله، IIS باید نصب شده باشد.

در ابتدا به قسمت Control Panel > Administrative Tools > Internet Information Service (IIS) رفته و در قسمت Web Site یک سایت جدید می سازیم در قسمت description نام سایت را وارد می کنیم.

در قسمت IP Address and Port setting ، در IP address سیستم سرور وب سایت (در این مورد همین ماشین) را وارد کرده، در قسمت مربوط به پورت، شماره پورت سایت و در قسمتHost Header نیز آدرس host را وارد می کنیم.

در قسمت بعد path فایل های سرور وب را وارد می کنیم و دکمه Next را کلیلک می کنیم .

در نهایت، دکمه Finish را کلیلک می کنیم.

اعمال تغییرات بر روی DNS برای ارتباط با IIS

در ابتدا به قسمت Control Panel > Administrative Tools >DNS می رویم . در این قسمت لازم است ، یک zone جدید در ارتباط با سایت ایجاد شده در IIS تعریف کنیم .

برای این کار در قسمت نام ماشین، روی Forward Lookup Zone کلیک راست کرده ، New zone را انتخاب می کنیم .این عمل برای این انجام می شود که آدرس IP ماشین، با آدرس هاست ، resolve شود.

در قسمت بعد، گزینه Primary Zone را انتخاب می کنیم و در قسمت Zone name ، نام سایت را بصورت کامل وارد می کنیم و Next را کلیک می کنیم.
در قسمت zone file گزینه پیش فرض را انتخاب می کنیم و در قسمت بعد Dynamic Update، ، گزینهDo not Allow Dynamic Update .را انتخاب می کنیم. Dynamic Update گزینه ای است که به DNS Client این امکان را می دهد که بصورت دینامیک ، از طریق یک DNS Server به روز شود .گزینه اول، هنگای فعال است که Active Directory بر روی سرور نصب شده باشد .این قابلیت باعث می شود،تغییرات بطور اتوماتیک اعمال شود.

در گزینه دوم، تغییرات از تمامی DNS Clients قبول شده و چون ممکن است از منابع نا شناخته و نا امن این تغییرات ارسال شود، یک نقطه ضعف امنیتی محسوب شده و توصیه نمی شود.گزینه سوم گزینه پیش فرض است که در اینجا ما آن را انتخاب می کنیم .
در قسمت بعد، نیاز است تا Host جدیدی در ارتباط با این domain بسازیم .برای این کار روی نام zone کلیک راست کرده و گزینه New Host را انتخاب می کنیم.
در قسمت IP Address ، آدرس IP مربوط به DNS را وارد می کنیم و Add Host را کلیک می کنیم.در نهایت، برای اعمال تغییرات انجام شده، این سرویس را مجددا راه اندازی می کنیم.
نکته : بدلیل اینکه در حال حاضر DNS هم روی همین ماشین Local نصب شده است پس DNS IP هم برابر با همان IP ماشین خواهد بود.

نصبCertificate Serviceوایجاد یکCA

در ابتدا به قسمت Control Panel > Add/Remove Programs > Add/Remove Windows Components می رویم.

چک باکس Certificate Services را فعال کرده و سپس Next را کلیک می کنیم.
بر روی صفحه ویزارد Certification Authority Types برای نوع CA، Stand-alone root CA را انتخاب می کنیم .همچنین چک باکس Advanced options را فعال می کنیم. قسمت Enterprise را هنگامی می توانیم استفاده کنیم که سرویس Active Directory نصب شده باشد .در این حالت اطلاعاتی که نیاز است، از طریق سیستم Active Directory وارد شده و سیستم، با Active Directory در ارتباط خواهد بود .تفاوت root و subordinate در این است که CA Subordinate تابعی از CA root است .سپس Next را کلیک می کنیم.
در صفحه Public and Private Key Pair قسمت "Microsoft Enhanced Cryptographic Provider v1.0" را انتخاب می کنیم . میتوان طول کلید پیش فرض ۱۰۲۴ را به عنوان Key length انتخاب کرد. سپسNext را کلیک می کنیم.

به این نکته باید توجه داشت که هر چه طول کلید بیشتر شود کلید بیشتر شود ، در زمان تبادل اطلاعات امنیت بیشتری خواهیم داشت و احتمال کشف کلید توسط Attacker ه ا کمتر خوا هد شد . در صفحه CA Identifying Information قسمت‌های موردنیاز را به شکل مناسب پر می کنیم. باید توجه داشت که common name ای که برای CA انتخاب می کنیم باید با نام DNS ، برابرباشد. سپس Next را کلیک می کنیم. در صفحه Certificate DataBase Settingمکان پیش فرض را انتخاب می کنیم. سپس Next را کلیک می کنیم و نهایتا کار را در این قسمت به پاین می رسانیم.

ایجاد یک Request از طرف وب سرور، برای دریافت Certificate از CA IIS یک WebPage برای درخواست Request دارد که از طریق آدرس زیر قابل اجراست:
Control Panel > Administrative Tools > Internet Information CertSRV Service> Default Web Site را Browse می کنیم.
نکته : از این صفحه همچنین می توانیم برای درخواست یک Certificate جهت e-mail client،WebBrowser و برنامه‌های دیگر استفاده کنیم.
ابتدا گزینه Request a certificate را انتخاب کرده و در مرحله بعد request advanced certificate را انتخاب می کنیم.

در این قسمت گزینه... Submit a certificate request by را انتخاب کرده و در مرحله بعد محتوای فایل Request ایجاد شده با فرمت txt. را در اینجا کپی می کنیم و در آخر Request را Submit می کنیم . سپس در Certificate Authority در قسمت Pending درخواست جدید را Issue می کنیم . Request در قسمت Issued Certificate قرار خواهد گرفت.

بدین ترتیب درخواستی که از طرف IIS برای دریافت Certificate به CA رسیده ، تایید و Certificate صادر خواهد شد.سپس روی Request مورد نظر دوبار کلیک کرده و در پنجره Details ، Certificate را انتخاب می کنیم و بعد گزینه Copy to File را انتخاب می کنیم. در قسمت Export file format ، فرمت - Based 64 encoded x.509 (.CER) را فعال می کنیم X509. استانداردی برای تعریف یک DigitalCertificate است .همچنین بعنوان سیستم امضا در SSL مورد استفاده قرار می گیرد .

در سایت زیر می توان مستنداتی در رابطه با X 509 یافت:

http://dmoz.org/Computers/Security/Public_Key_Infrastructure/X. 509

در مرحله بعد آدرس و نام فایلCertificate را مشخص می نماییم و سپس ویزارد را به پایان می رسانیم. در مرحله بعد به IIS رفته و فایل export شده را به IIS معرفی می کنیم .بدین طریق که بر روی IIS کلیک راست کرده Properties را انتخاب می کنیم .سپس به Directory Security رفته و گزینه Server Certificate را انتخاب می کنیم .در قسمت Pending Certificate Requestگزینه اول را انتخاب می کنیم.

در قسمت بعد نام فایلی را که export کرده ایم وارد کرده و پورت پیش فرض ۴۴۳ را انتخاب می کنیم و با کلیک Finish پروسه نصب و راه اندازی ، به اتمام می رسد .با browser خود ، آدرس سایت را بصورت https://your-site.com وارد می کنیم.

ضمیمه ۲ : پراکسی

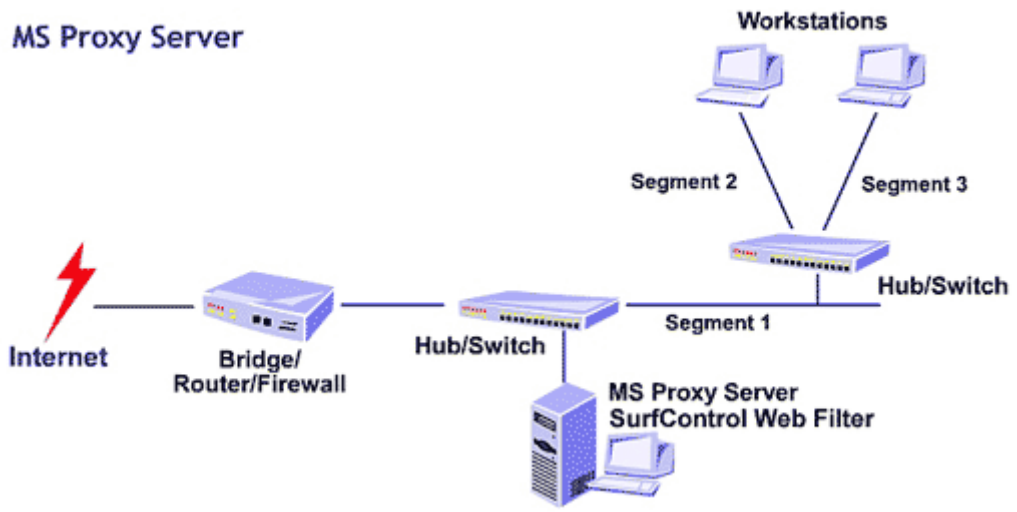
پراکسی چیست؟

در دنیای امنیت شبکه، افراد از عبارت «پراکسی» برای خیلی چیزها استفاده می کنند. اما عموماً، پراکسی ابزار است که بسته های دیتای اینترنتی را در مسیر دریافت‌می کند

آن دیتا را می سنجد و عملیاتی برای سیستم مقصد آن دیتا انجام می دهد. در اینجا از پراکسی به معنی پروسه ای یاد می شود که در راه ترافیک شبکه ای قبل از اینکه به شبکه وارد یا از آن خارج شود، قرار می گیرد و آن را می سنجد تا ببیند با سیاست های امنیتی شما مطابقت دارد و سپس مشخص می کند که آیا به آن اجازه عبور از فایروال را بدهد یا خیر. بسته های مورد قبول به سرور مورد نظر ارسال و بسته های ردشده دور ریخته می شوند.

پراکسی چه چیزی نیست؟

پراکسی ها بعضی اوقات با دو نوع فایروال اشتباه می شوند « Packet filter و Stateful packet filter» که البته هر کدام از روش ها مزایا و معایبی دارد، زیرا همیشه یک مصالحه بین کارایی و امنیت وجود دارد.



پراکسی با Packet filter تفاوت دارد

ابتدایی ترین روش صدور اجازه عبور به ترافیک بر اساس TCP/IP این نوع فیلتر بود. این نوع فیلتر بین دو یا بیشتر رابط شبکه قرار می گیرد و اطلاعات آدرس را در IP header ترافیک دیتایی که بین آنها عبور می کند، پیمایش می کند. اطلاعاتی که این نوع فیلتر ارزیابی می کند عموماً شامل آدرس و پورت منبع و مقصد می شود. این فیلتر بسته به پورت و منبع و مقصد دیتا و بر اساس قوانین ایجاد شده توسط مدیر شبکه بسته را می پذیرد یا نمی پذیرد. مزیت اصلی این نوع فیلتر سریع بودن آن است چرا که header، تمام آن چیزی است که سنجیده می شود. و عیب اصلی ان این است

که هرگز آنچه را که در بسته وجود دارد نمی بیند و به محتوای آسیب رسان اجازه عبور از فایروال را می دهد. بعلاوه، این نوع فیلتر با هر بسته بعنوان یک واحد مستقل رفتار می کند و وضعیت (State) ارتباط را دنبال نمی کند.

پراکسی با Stateful packet filter تفاوت دارد

این فیلتر اعمال فیلتر نوع قبل را انجام می دهد، بعلاوه اینکه بررسی می کند کدام کامپیوتر در حال ارسال چه دیتایی است و چه نوع دیتایی باید بیاید. این اطلاعات بعنوان وضعیت (State) شناخته می شود.

پروتکل ارتباطی TCP/IP به ترتیبی از ارتباط برای برقراری یک مکالمه بین کامپیوترها نیاز دارد. در آغاز یک ارتباط TCP/IP عادی، کامپیوتر A سعی می کند با ارسال یک بسته SYN (synchronize) به کامپیوتر B ارتباط را برقرار کند. کامپیوتر B در جواب یک بسته SYN/ACK (Acknowledgement)) برمی گرداند، و کامپیوتر A یک ACK به کامپیوتر B می فرستد و به این ترتیب ارتباط برقرار می شود. TCP اجازه وضعیتهای دیگر، مثلاً FIN (finish) برای نشان دادن آخرین بسته در یک ارتباط را نیز می دهد.

هکرها در مرحله آماده سازی برای حمله، به جمع آوری اطلاعات در مورد سیستم شما می پردازند. یک روش معمول ارسال یک بسته در یک وضعیت غلط به منظوری خاص است. برای مثال، یک بسته با عنوان پاسخ (Reply) به سیستمی که تقاضایی نکرده، می فرستند. معمولاً، کامپیوتر دریافت کننده بیاید پیامی بفرستد و بگوید "I don't understand" . به این ترتیب، به هکر نشان می دهد که وجود دارد، و آمادگی برقراری ارتباط دارد. بعلاوه، قالب پاسخ می تواند سیستم عامل مورد استفاده را نیز مشخص کند، و برای یک هکر گامی به جلو باشد. یک فیلتر Stateful packet منطق یک ارتباط TCP/IP را می فهمد و می تواند یک "Reply" را که پاسخ به یک تقاضا نیست، مسدود کند ـــ آنچه که یک فیلتر packet ردگیری نمی کند و نمی تواند انجام دهد. فیلترهای Stateful packet می توانند در همان لحظه قواعدی را مبنی بر اینکه بسته مورد انتظار در یک ارتباط عادی چگونه باید بنظر رسد، برای پذیرش یا رد بسته بعدی تعیین کنند. فایده این کار امنیت محکم تر است. این امنیت محکم تر، بهرحال، تا حدی باعث کاستن از کارایی می شود. نگاهداری لیست قواعد ارتباط

بصورت پویا برای هر ارتباط و فیلترکردن دیتای بیشتر، حجم پردازشی بیشتری به این نوع فیلتر اضافه می کند.

پراکسی ها یا Application Gateways

Application Gateways که عموماً پراکسی نامیده می شود، پیشرفته ترین روش استفاده شده برای کنترل ترافیک عبوری از فایروال ها هستند. پراکسی بین کلاینت و سرور قرار می گیرد و تمام جوانب گفتگوی بین آنها را برای تایید تبعیت از قوانین برقرار شده، می سنجد. پراکسی بار واقعی تمام بسته های عبوری بین سرور و کلاینت را می سنجد، و می تواند چیزهایی را که سیاستهای امنیتی را نقض می کنند، تغییر دهد یا محروم کند. توجه کنید که فیلترهای بسته ها فقط headerها را می سنجند، در حالیکه پراکسی ها محتوای بسته را با مسدود کردن کدهای آسیب رسان همچون فایلهای اجرایی، اپلت های جاوا، ActiveX و ... غربال می کنند.

پراکسی ها همچنین محتوا را برای اطمینان از اینکه با استانداردهای پروتکل مطابقت دارند، می سنجند. برای مثال، بعضی اَشکال حمله کامپیوتری شامل ارسال متاکاراکترها برای فریفتن سیستم قربانی است؛ حمله های دیگر شامل تحت تاثیر قراردادن سیستم با دیتای بسیار زیاد است. پراکسی ها می توانند کاراکترهای غیرقانونی یا رشته های خیلی طولانی را مشخص و مسدود کنند. بعلاوه، پراکسی ها تمام اعمال فیلترهای ذکرشده را انجام می دهند. بدلیل تمام این مزیتها، پراکسی ها بعنوان یکی از امن ترین روشهای عبور ترافیک شناخته می شوند. آنها در پردازش ترافیک از فایروالها کندتر هستند زیرا کل بسته ها را پیمایش می کنند. بهرحال «کندتر» بودن یک عبارت نسبی است.

آیا واقعاً کند است؟ کارایی پراکسی بمراتب سریعتر از کارایی اتصال اینترنت کاربران خانگی و سازمانهاست. معمولاً خود اتصال اینترنت گلوگاه سرعت هر شبکه ای است. پراکسی ها باعث کندی سرعت ترافیک در تست های آزمایشگاهی می شوند اما باعث کندی سرعت دریافت کاربران نمی شوند. در شماره بعد بیشتر به پراکسی خواهیم پرداخت.

مزایای پراکسی‌ها بعنوان ابزاری برای امنیت :

- با مسدود کردن روش‌های معمول مورد استفاده در حمله‌ها، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با پنهان کردن جزئیات سرورهای شبکه شما از اینترنت عمومی، هک‌کردن شبکه شما را مشکل‌تر می‌کنند.
- با جلوگیری از ورود محتویات ناخواسته و نامناسب به شبکه شما، استفاده از پهنای باند شبکه را بهبود می‌بخشند.
- با ممانعت از یک هکر برای استفاده از شبکه شما بعنوان نقطه شروعی برای حمله دیگر، از میزان این نوع مشارکت می‌کاهند.
- با فراهم‌آوردن ابزار و پیش‌فرض‌هایی برای مدیر شبکه شما که می‌توانند بطور گسترده‌ای استفاده شوند، می‌توانند مدیریت شبکه شما را آسان سازند.

بطور مختصر می‌توان این مزایا را اینگونه بیان کرد؛ پراکسی‌ها به شما کمک می‌کنند که شبکه‌تان را با امنیت بیشتر، موثرتر و اقتصادی‌تر مورد استفاده قرار دهید. بهرحال در ارزیابی یک فایروال، این مزایا به فواید اساسی تبدیل می‌شوند که توجه جدی را می‌طلبند.

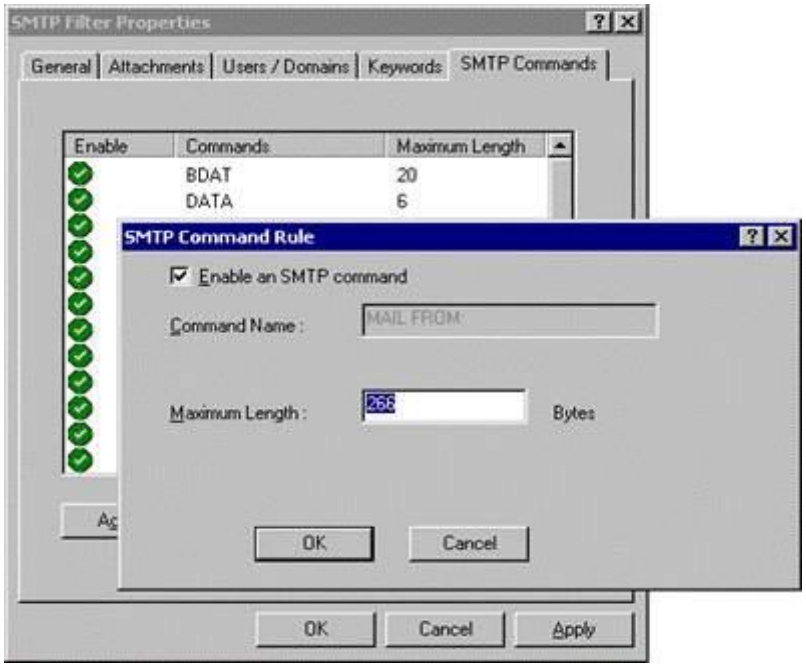
برخی انواع پراکسی

تا کنون به پراکسی بصورت یک کلاس عمومی تکنولوژی پرداختیم. در واقع، انواع مختلف پراکسی وجود دارد که هرکدام با نوع متفاوتی از ترافیک اینترنت سروکار دارند. در بخش بعد به چند نوع آن اشاره می‌کنیم و شرح می‌دهیم که هرکدام در مقابل چه نوع حمله‌ای مقاومت می‌کند.

البته پراکسی‌ها تنظیمات و ویژگی‌های زیادی دارند. ترکیب پراکسی‌ها و سایر ابزار مدیریت فایروال‌ها به مدیران شبکه شما قدرت کنترل امنیت شبکه تا بیشترین جزئیات را می‌دهد.

در ادامه به پراکسی‌های زیر اشاره خواهیم کرد:

- SMTP Proxy
- HTTP Proxy
- FTP Proxy
- DNS Proxy



SMTP Proxy

پراکسی SMTP (Simple Mail Transport Protocol) محتویات ایمیل‌های وارد شونده و خارج‌شونده را برای محافظت از شبکه شما در مقابل خطر بررسی می‌کند. بعضی از تواناییهای آن اینها هستند:

- **مشخص کردن بیشترین تعداد دریافت‌کنندگان پیام** : این اولین سطح دفاع علیه اسپم (هرزنامه) است که اغلب به صدها یا حتی هزاران دریافت‌کننده ارسال می‌شود.

- **مشخص کردن بزرگترین اندازه پیام:** این به سرور ایمیل کمک می‌کند تا از بار اضافی و حملات بمباران توسط ایمیل جلوگیری کند و با این ترتیب می‌توانید به درستی از پهنای باند و منابع سرور استفاده کنید.
- **اجازه دادن به کاراکترهای مشخص در آدرسهای ایمیل آنطور که در استانداردهای اینترنت پذیرفته شده است:** چنانچه قبلاً اشاره شد، بعضی حمله‌ها بستگی به ارسال کاراکترهای غیرقانونی در آدرسها دارد. پراکسی می‌تواند طوری تنظیم شود که بجز به کاراکترهای مناسب به بقیه اجازه عبور ندهد.
- **فیلترکردن محتوا برای جلوگیری از انواعی محتویات اجرایی:** معمول‌ترین روش ارسال ویروس، کرم و اسب تروا فرستادن آنها در پیوست‌های به ظاهر بی‌ضرر ایمیل است. پراکسی SMTP می‌تواند این حمله‌ها را در یک ایمیل از طریق نام و نوع، مشخص و جلوگیری کند، تا آنها هرگز به شبکه شما وارد نشوند.
- **فیلترکردن الگوهای آدرس برای ایمیل‌های مقبول \مردود:** هر ایمیل شامل آدرسی است که نشان‌دهنده منبع آن است. اگر یک آدرس مشخص شبکه شما را با تعداد بیشماری از ایمیل مورد حمله قرار دهد، پراکسی می‌تواند هر چیزی از آن آدرس اینترنتی را محدود کند. در بسیاری موارد، پراکسی می‌تواند تشخیص دهد چه موقع یک هکر آدرس خود را جعل کرده است. از آنجا که پنهان کردن آدرس بازگشت تنها دلایل خصمانه دارد، پراکسی می‌تواند طوری تنظیم شود که بطور خودکار ایمیل جعلی را مسدود کند.
- **فیلترکردن Headerهای ایمیل:** Headerها شامل دیتای انتقال مانند اینکه ایمیل از طرف کیست، برای کیست و غیره هستند. هکرها راه‌های زیادی برای دستکاری اطلاعات Header برای حمله به سرورهای ایمیل یافته‌اند. پراکسی مطمئن می‌شود که Headerها با پروتکل‌های اینترنتی صحیح تناسب دارند و ایمیل‌های دربردارنده headerهای تغییرشکل‌داده را مردود می‌کنند. پراکسی با اعمال سختگیرانه استانداردهای ایمیل نرمال، می‌تواند برخی حمله‌های آتی را نیز مسدود کند.
- **تغییردادن یا پنهان‌کردن نامهای دامنه و IDهای پیام‌ها:** ایمیل‌هایی که شما می‌فرستید نیز مانند آنهایی که دریافت می‌کنید، دربردارنده دیتای header هستند. این دیتا بیش از آنچه شما می‌خواهید دیگران درباره امور داخلی شبکه شما بدانند، اطلاعات دربردارند. پراکسی SMTP می‌تواند بعضی از این اطلاعات را پنهان کند یا

تغییر دهد تا شبکه شما اطلاعات کمی در اختیار هکرهایی قرار دهد که برای وارد شدن به شبکه شما دنبال سرنخ می‌گردند.

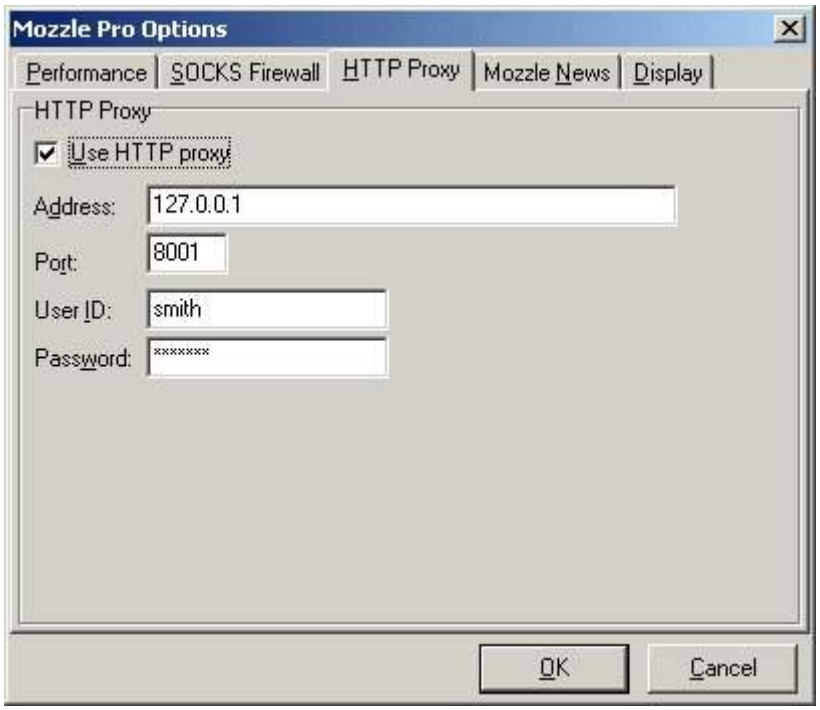
HTTP Proxy

این پراکسی بر ترافیک داخل شونده و خارج شونده از شبکه شما که توسط کاربرانتان برای دسترسی به World Wide Web ایجاد شده، نظارت می کند. این پراکسی برای مراقبت از کلاینت های وب شما و سایر برنامه ها که به دسترسی به وب از طریق اینترنت متکی هستند و نیز حملات برپایه HTML، محتوا را فیلتر می کند. بعضی از قابلیتهای آن اینها هستند:

- **برداشتن اطلاعات اتصال کلاینت:** این پراکسی می تواند آن قسمت از دیتای header را که نسخه سیستم عامل، نام و نسخه مرورگر، حتی آخرین صفحه وب دیده شده را فاش می کند، بردارد. در بعضی موارد، این اطلاعات حساس است، بنابراین چرا فاش شوند؟
- **تحمیل تابعیت کامل از استانداردهای مقررشده برای ترافیک وب:** در بسیاری از حمله ها، هکرها بسته های تغییرشکل داده شده را ارسال می کنند که باعث دستکاری عناصر دیگر صفحه وب می شوند، یا بصورتی دیگر با استفاده از رویکردی که ایجادکنندگان مرورگر پیش بینی نمی کردند، وارد می شوند. پراکسی HTTP این اطلاعات بی معنی را نمی پذیرد. ترافیک وب باید از استانداردهای وب رسمی پیروی کند، وگرنه پراکسی ارتباط را قطع می کند.
- **فیلترکردن محتوای از نوع MIME** : الگوهای MIME به مرورگر وب کمک می کنند تا بداند چگونه محتوا را تفسیر کند تا با یک تصویرگرافیکی بصورت یک گرافیک رفتار شود، یا wav. فایل بعنوان صوت پخش شود، متن نمایش داده شود و غیره. بسیاری حمله های وب بسته هایی هستند که در مورد الگوی MIME خود دروغ می گویند یا الگوی آن را مشخص نمی کنند. پراکسی HTTP این فعالیت مشکوک را تشخیص می دهد و چنین ترافیک دیتایی را متوقف می کند.
- **فیلترکردن کنترلهای Java و ActiveX**: برنامه نویسان از Java و ActiveX برای ایجاد برنامه های کوچک بهره می گیرند تا در درون یک مرورگر وب اجراء شوند (مثلاً اگر فردی یک صفحه وب مربوط به امور جنسی را مشاهده می کند، یک اسکریپت ActiveX روی آن صفحه می تواند بصورت خودکار آن صفحه را صفحه

خانگی مرورگر آن فرد نماید). پراکسی می تواند این برنامه ها را مسدود کند و به این ترتیب جلوی بسیاری از حمله ها را بگیرد.

- **برداشتن کوکی ها:** پراکسی HTTP می تواند جلوی ورود تمام کوکی ها را بگیرد تا اطلاعات خصوصی شبکه شما را حفظ کند.
- **برداشتن Headerهای ناشناس:** پراکسی HTTP ، از headerهای HTTP که از استاندارد پیروی نمی کنند، ممانعت بعمل می آورد. یعنی که، بجای مجبور بودن به تشخیص حمله های برپایه علائمشان، پراکسی براحتی ترافیکی را که خارج از قاعده باشد، دور می ریزد. این رویکرد ساده از شما در مقابل تکنیک های حمله های ناشناس دفاع می کند.
- **فیلترکردن محتوا:** دادگاه ها مقررکرده اند که تمام کارمندان حق برخورداری از یک محیط کاری غیر خصمانه را دارند. بعضی عملیات تجاری نشان می دهد که بعضی موارد روی وب جایگاهی در شبکه های شرکت ها ندارند. پراکسی HTTP سیاست امنیتی شرکت شما را وادار می کند که توجه کند چه محتویاتی مورد پذیرش در محیط کاریتان است و چه هنگام استفاده نامناسب از اینترنت در یک محیط کاری باعث کاستن از بازده کاری می شود. بعلاوه، پراکسی HTTP می تواند سستی ناشی از فضای سایبر را کم کند. گروه های مشخصی از وب سایتها که باعث کم کردن تمرکز کارمندان از کارشان می شود، می توانند غیرقابل دسترس شوند.

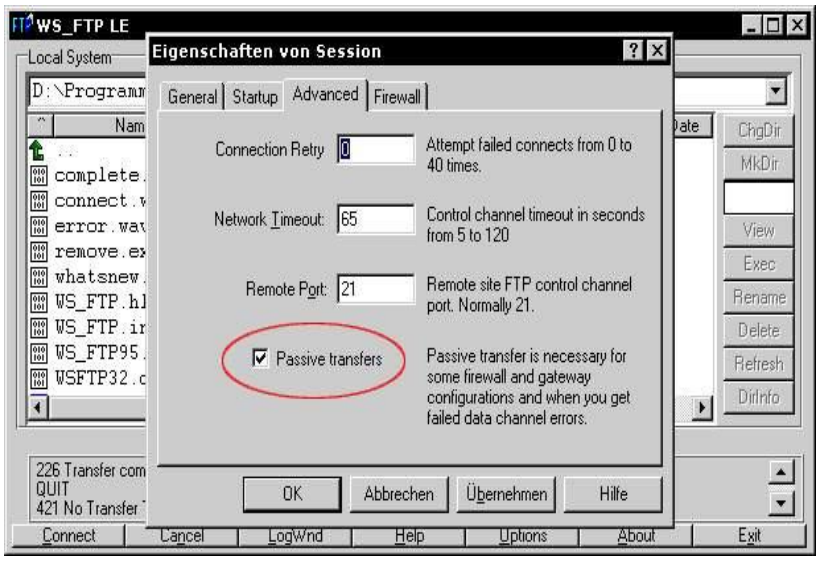


FTP Proxy

بسیاری از سازمان ها از اینترنت برای انتقال فایل های دیتای بزرگ از جایی به جایی دیگر استفاده می کنند. در حالیکه فایل های کوچک تر می توانند بعنوان پیوست های ایمیل منتقل شوند، فایل های بزرگ تر توسط FTP (File Transfer Protocol) فرستاده می شوند. بدلیل اینکه سرورهای FTP فضایی را برای ذخیره فایل ها آماده می کنند، هکرها علاقه زیادی به دسترسی به این سرورها دارند.

پراکسی FTP معمولاً این امکانات را دارد:

- **محدودکردن ارتباطات از بیرون به «فقط خواندنی»:** این عمل به شما اجازه می دهد که فایل ها را در دسترس عموم قرار دهید، بدون اینکه توانایی نوشتن فایل روی سرورتان را بدهید.
- **محدود کردن ارتباطات به بیرون به «فقط خواندنی»:** این عمل از نوشتن فایل های محرمانه شرکت به سرورهای FTP خارج از شبکه داخلی توسط کاربران جلوگیری می کند.
- **مشخص کردن زمانی ثانیه های انقضای زمانی:** این عمل به سرور شما اجازه می دهد که قبل از حالت تعلیق و یا Idle request ارتباط را قطع کند.
- **ازکارانداختن فرمان FTP SITE** : این از حمله هایی جلوگیری می کند که طی آن هکر فضایی از سرور شما را تسخیر می کند تا با استفاده از سیستم شما حمله بعدی خودش را پایه ریزی می کند.



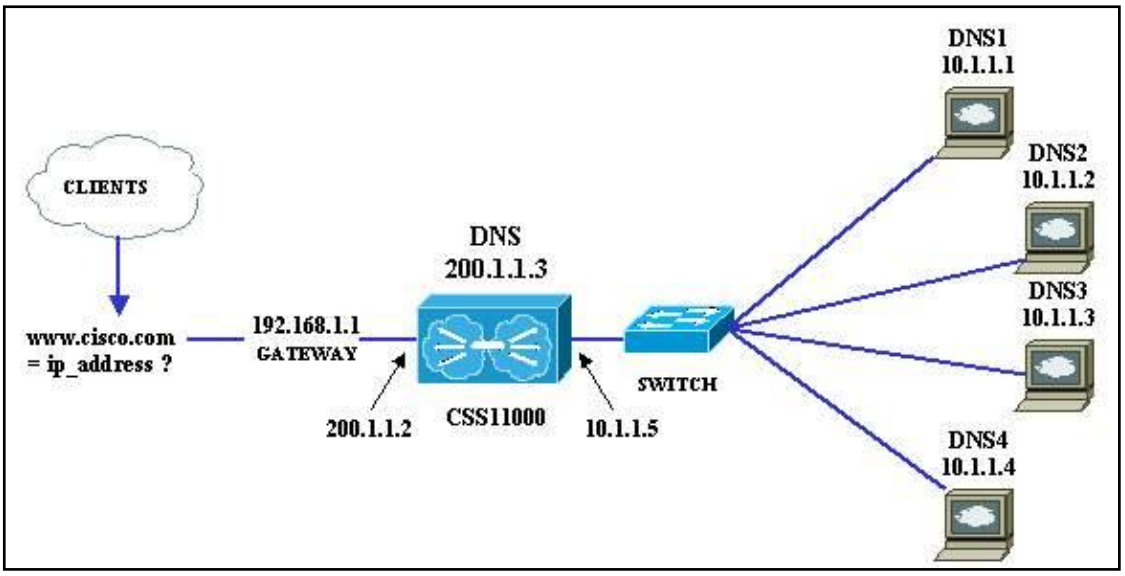
DNS Proxy

DNS (Domain Name Server) شاید به اندازه HTTP یا SMTP شناخته شده نیست، اما چیزی است که به شما این امکان را می دهد که نامی را مانند http://www.ircert.com در مرورگر وب خود تایپ کنید و وارد این سایت شوید – بدون توجه به اینکه از کجای دنیا به اینترنت متصل شده اید. بمنظور تعیین موقعیت و نمایش منابعی که شما از اینترنت درخواست می کنید، DNS نام های دامنه هایی را که می توانیم براحتی بخاطر بسپاریم به آدرس IP هایی که کامپیوترها قادر به درک

آن هستند، تبدیل می کند. در اصل این یک پایگاه داده است که در تمام اینترنت توزیع شده است و توسط نام دامنه ها فهرست شده است.

بهرحال، این حقیقت که این سرورها در تمام دنیا با مشغولیت زیاد در حال پاسخ دادن به تقاضاها برای صفحات وب هستند، به هکرها امکان تعامل و ارسال دیتا به این سرورها را برای درگیرکردن آنها می دهد. حمله های برپایه DNS هنوز خیلی شناخته شده نیستند، زیرا به سطحی از پیچیدگی فنی نیاز دارند که بیشتر هکرها نمی توانند به آن برسند. بهرحال، بعضی تکنیک های هک که میشناسیم باعث می شوند هکرها کنترل کامل را بدست گیرند. بعضی قابلیت های پراکسی DNS می تواند موارد زیر باشد:

- **تضمین انطباق پروتکلی:** یک کلاس تکنیکی بالای اکسپلویت می تواند لایه Transport را که تقاضاها و پاسخ های DNS را انتقال می دهد به یک ابزار خطرناک تبدیل کند. این نوع از حمله ها بسته هایی تغییرشکل داده شده بمنظور انتقال کد آسیب رسان ایجاد می کنند. پراکسی DNS، headerهای بسته های DNS را بررسی می کند و بسته هایی را که بصورت ناصحیح ساخته شده اند، دور می ریزد و به این ترتیب جلوی بسیاری از انواع سوء استفاده را می گیرد.
- **فیلترکردن محتوای headerها بصورت گزینشی:** DNS در سال ۱۹۸۴ ایجاد شده و از آن موقع بهبود یافته است. بعضی از حمله های DNS بر ویژگی هایی تکیه می کنند که هنوز تایید نشده اند. پراکسی DNS می تواند محتوای header تقاضاهای DNS را بررسی کند و تقاضاهایی را که کلاس، نوع یا طول header غیرعادی دارند، مسدود کند.


DNS1
10.1.1.1
DNS2
10.1.1.2
DNS3
10.1.1.3
DNS4
10.1.1.4
CLIENTS
DNS
200.1.1.3
www.cisco.com
= ip_address ?
192.168.1.1
GATEWAY
200.1.1.2
CSS11000
10.1.1.5
SWITCH

واژه نامه :

1. Individual Messages
2. Authenticate
3. Handshaking
4. Cipher Preferences
5. Master Key
6. Public Key
7. Challenge
8. Public-Key Certificate
9. Transport Layer Security
10. Wireless TLS
11. Wireless Application Protocol
12. Certificate
13. Certificate Authority
14. Symmetric Key

فهرست منابع :

- **منابع اینترنتی:**

http://www.webopedia.com/TERM/S/SSL.html
http://www.rsasecurity.com/
http://www.webopedia.com/TERM/S/S_HTTP.htm
http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO
http://www.verisign.com/products-services
http://www.fekrinejat.com/
http://www.hamkelasy.com/
http://www.ircert.com/
http://www.persiantop.com/
http://www.ostadonline.com/
http://www.parslan.com/
http://www.ouriran.com/
http://www.yazdit.mihanblog.com/
http://www.ksajadi.com/
http://www.golha.ir/
http://www.wikipedia.com/
http://www.sgnetway.com/
http://www.reporter.ir/
http://www.mcs-8051.com

- **منابع فارسی**

قدیر پور رستم ، مدل های اعتماد بر بستر کلید عمومی ، کتاب مقالات چهارمین همایش ملی دانشجویی،انجمن کامپیوتر ایران ، ۱۳۸۱