بسمه تعالی

موضوع تحقیق: امنیت شبکه های بی سیم

Wi-Fi

نام درس : امنیت شبکه های کامپیوتر

نام استاد : آقای رمضانی

دانشگاه جامع علمی کاربردی/ فناوری اطلاعات

نام دانشجو : اصغرجاویدمیاب

www.itport.ir

تابستان 1391

فهرست

چکیده :

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی هستند که توانسته اند توجه بسیاری را بسوی خود جلب نمایند و عده ای را نیز مسحور خود نموده اند. هرچند این تکنولوژی جذابیت و موارد کاربرد بالایی دارد ولی مهمترین مرحله که تعیین کننده میزان رضایت از آن را بدنبال خواهد داشت ارزیابی نیاز ها و توقعات و مقایسه آن با امکانات و قابلیت های این تکنولوژی است.امروزه امنیت شبکه یک مساله مهم برای ادارات وشرکتهای دولتی وسازمانهای بزرگ وکوچک است تهدیدهای پیشرفته از تروریست های فضای سایبر کارمندان ناراضی وهکرهای رویکردی سیستمانیکا برای امنیت شبکه می طلبد. در بررسی روشما واستاندارد های امن سازی شبکه های محلی بی سیم مبتنی براستاندارد IEEE802.11 می پردازیم .با طرح قابلیت امنیتی این استاندارد می توان از محدودیت ان آگاه شد استاندارد 802011 سروس های مجزا و مشخصی را برای تامین یک محیط امن در اختیار قرار میدهد دراین سروس اغلب توسط پروتکلWEPتامین میگرددوظیفه آن امن سازی میان مخدوم ونقاط استرسی بی سیم است در حال حاضر تنها پروتکل که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم براساس استاندارد 802.11 فراهم میکند WEPاست این پروتکل نوع استفاده از آن

همواره امکان نفوذ به شبکه های بی سیم راهر نحوی ولو سخت وپیچیده فراهم میکنـد و بسـیار از حمـلات برروی شبکه های سیمی دارای اشتراک است .

فصل اول : شبکه های بی سیم و تکنولوژی WI-FI

1-1)شبکه های بی سیم و تکنولوژی WI-FI

بـا گسـترش روز افـزون فـن آوری اطلاعـات وپیشـرفته شـدن شـبکه هـای کـامپیوتری ونیـاز بـه تبـادل اطلاعـات بـا سـرعت بـالا احتیـاج بـه ایـن تکنولـوژی بـیش از پـیش محسـوس مـی باشـد.ارتباط شـبکه هـای کـامپیوتری بـه روش سـیمی در مسـافت هـای طـولانی دارای محـدودیت هـای سـرعت ارتبـاط و مسـتلزم هزینـه هـای زیـاد اسـت.لذا بـرای حـل ایـن مشـکل اندیشـمندان درصـدد برآمدنـد تـااز طریـق شـبکه هـای بـی سـیم محـدودیت هـای موجـود را رفـع کنند.البتـه لازم بـه ذکـر اسـت شـبکه هـای بـی سـیم دارای محـدودیت فاصـله مـی باشـند بـه گونـه ای کـه حـداکثر فاصله پوشش شبکه هـای بیسـیم ۱۲۰ الـی ۱۵۰ کیلـومتر اسـت ولـی در مقایسـه بـا شـبکه هـای سـیمی مزیـت هـای قابل توجهی دارند. برای نمونه میتـوان بـه سـرعت بـالا نداشـتن شـارژ ماهیانـه هزینـه هـای جـاری اشـاره کـرد. سـرعت پیشـرفت ایـن نـوع شـبکه هـا بـه گونـه ای بـوده اسـت کـه در حـال حاضـر اکثـر ادارات وسـازمان هـای دولتـی ویـا موسسـات خصوصـی بـه طـور چشـم گیـری از ایـن تکنولـوژی اسـتقبال کردنـد. توضـیح دیگـر اینکـه :شـبکه هـای بـی سیم با استفاده از تکنولـوژی Wi-Fi و براسـاس امـواج کـار میکنـد کـه ایـن امـواج دارای فرکـانس هـایی هسـتند کـه ISM نامیده میشـوند. فرکـانس هـای ISMبـه عنـوان فرکـانس هـای آزاد در دنیـا معرفـی شـده و احتیـاج بـه داشـتن هیچگونـه مجـوز یـا مـدرک از سـازمان خاصـی نمـی باشـد. یکـی دیگـر از مزایـای برتـر شـبکه هـای بـی سـیم امکـان استفاده از این شبکه ها در جاهـایی کـه حتـی از امکانـات مخـابراتی نیـز بـی بهـره انـد، بـه طـور مثـال بـه وسـیله ایـن ارتباطات مـی تـوان خطـوط تلفـن را بـه محـل هـای فاقـد امکانـات منتقـل کـرد ویـا مـی تـوان تصـاویر را بـه صـورت

واقعی انتقال داد. شاید مهمترین مزیت شبکه های بی سیم قابلیت متحرک بودن آن می باشد بدین معنی که کاربر میتواند بدون نیاز به استفاده از کابل به شبکه متصل شده واطلاعات مورد نظر رادریافت یا انتقال دهد. همین امر باعث صرفه جویی در زمان و هزینه کابل کشی نیز خواهد شد . به طور مثال استفاده از این تکنولوژی در مراکزی چون هتل ها،رستوران ها،مدارس ودیگر سازمانهای دولتی یا خصوصی به سهولت می توان استفاده کرد. از مهمترین نگرانیهای شبکه های بی سیم حفاظت اطلاعات این نوع شبکه هاست که این امر نیز پیش بینی شده وراهکار های مطمئن تعبیه شده است که در این صورت استفاده از این لایه های امنیتی می توان گفت شبکه های بی سیم قطعا از شبکه های سیمی امن تر خواهند بود.

1-2) Wi-Fi چیست و چگونه کار می کند؟

در فرودگاه، هتل، رستوران، کتابخانه و یا حتی دفتر کار، امروزه دیگر در هر کجا که تصور کنید ممکن است بتوانید به اینترنت متصل شوید. در آینده ای نزدیک شبکه های ارتباطی بدون سیم چنان گسترشی می یابند که در هر زمان و مکانی شاهد ارائه خدمات اینترنت بی سیم خواهید بود. به کمک شبکه هایی همچون Wi-Fi قادر خواهید بود تا رایانه های یک اطاق یا دفتر کار خود را به راحتی به یکدیگر متصل نمایید.

شبکه های ارتباطی بدون سیم همواره از امواج رادیویی استفاده می کنند. در این شبکه ها یک قطعه رایانه ای، اطلاعات را تبدیل به امواج رادیویی می نماید و آنها را از طریق آنتن ارسال می کند. در طرف دیگر یک روتر بدون سیم، با دریافت سیگنال های فوق و تبدیل آنها به اطلاعات اولیه، داده ها را برای رایانه قابل فهم خواهد ساخت.

به زبانی ساده، سیستم Wi-Fi را می توان به یک جفت واکی - تاکی که شما از آن برای مکالمه با دوستان خود استفاده می کنید تشبیه نمود. این لوازم، رادیوهای کوچک و ساده ای هستند که قادرند تا سیگنال های رادیویی را ارسال و دریافت نمایند. هنگامی که شما بوسیله آنها صحبت می کنید، میکروفون دستگاه، صدای شما را دریافت نموده و با تلفیق آن با امواج رادیویی، از طریق آنتن آنها را ارسال می کند.

در طرف دیگر، دستگاه مقصد، با دریافت سیگنال ارسال شده از طرف شما توسط آنتن، آنها را آشکار سازی نموده و از طریق بلندگوی دستگاه، صدای شما را پخش خواهد کرد. توان خروجی و یا قدرت فرستنده این گونه لوازم اغلب در حدود یک چهارم وات است و با این وصف، برد آنها چیزی در حدود ۵۰ تا ۱۰۰ متر می رسد.

حال فرض کنید بخواهید میان دو کامپیوتر به صورت یک شبکه و آن هم به شکل بدون سیم (همانند واکی - تاکی) ارتباط برقرار سازید. مشکل اساسی در این راه آن است که این لوازم از آن رو که جهت انتقال صوت ساخته شده اند، از نرخ سرعت انتقال کمی برخوردار هستند و نمی توانند حجم بالایی از داده ها را در زمان کوتاه منتقل کنند.

رادیوهایی که در سیستم Wi-Fi مورد استفاده قرار می گیرند، همانند مثال پیشین قابلیت ارسال و دریافت را دارا می باشند اما تفاوت اصلی آنها در این است که این رادیو ها قادر هستند تا اطلاعات به شکل صفر و یک دیجیتالی را به حالت امواج رادیویی تبدیل نمایند و سپس منتقل کنند.

در کل سه تفاوت عمده میان رادیوهای سیستم Wi-Fi و رادیوهای واکی - تاکی معمولی وجود دارد که به شرح زیر است:

۱) رادیوهای سیستم Wi-Fi با استاندارد های b802.11 و g802.11 کار می کنند و عمل ارسال و دریافت را بر روی فرکانس های 2.4 گیگاهرتزی و یا ۵ گیگا هرتزی انجام می دهند. اما واکی - تاکی های مذکور بر روی فرکانس ۴۹ مگاهرتزی کار می کنند.

۲) رادیوهای سیستم Wi-Fi از انواع مختلفی از تکنیک های کدگذاری اطلاعات بهره می برند که نتیجه آن افزایش نرخ سرعت تبادل داده ها خواهد بود. این روشها برای استاندارد a802.11 و g802.11 شامل تکنیک OFDM و برای استاندارد b802.11 شامل CCK می باشد.

۳) رادیو هایی کـه در سیسـتم Wi-Fi مـورد اسـتفاده قـرار مـی گیرنـد، قابلیـت تغییـر فرکـانس را دارا هسـتند. مزیـت این ویژگـی در آن اسـت کـه موجـب جلـوگیری از ایجـاد تـداخل کـار سیسـتم هـای مختلـف Wi-Fi در نزدیکـی هـم می شود.

بـه دلایلـی کـه ذکـر شـد، سیسـتم هـای رادیـویی Wi-Fi ظرفیـت و سـرعت انتقـال داده بـالاتری را نسـبت بـه رادیـو های واکـی - تـاکی دارنـد، ایـن سـرعت هـا بـرای اسـتاندارد b802.11 تـا ۱۱ مگابایـت بـر ثانیـه و بـرای a802.11 و g802.11 در حدود ۳۰ مگابایت بر ثانیه است.

1-3) ترکیب سیستم Wi-Fi با رایانه:

امروزه اغلـب رایانـه هـای لـپ تـاپ مجهـز بـه سیسـتم Wi-Fi داخلـی هسـتند و در غیـر ایـن صـورت نیازمنـد نصـب یک کارت Wi-Fi بر روی لـپ تـاپ و یـا رایانـه رومیـزی خـود خـواهیم بـود. شـما مـی توانیـد یـک کـارت Wi-Fi در سیسـتم a802.11 یـا b802.11 و یـا g802.11 تهیـه کنیـد کـه البتـه نـوع g802.11 نسـبت بـه تجهـزات b802.11 از سـرعت بـالاتری برخـوردار اسـت. بـرای لـپ تـاپ هـا ایـن تجهیـزات در قالـب کـارت هـای PCMCIA که در محل مخصوص خود نصـب مـی شـوند و یـا بـه صـورت اتصـال خـارجی از طریـق یـک درگـاه USB عرضـه مـی شوند.

برای رایانه های رومیـزی، مـی توانیـد از کـارت هـای PCI و یـا درگـاه USB بـرای ایـن منظـور اسـتفاده کنیـد. پـس از نصب این تجهیزات کاربر قادر است تا در مکان هـایی کـه اینترنـت بـه شـکل بـدون سـیم ارائـه مـی شـود بـا داشـتن یک اشتراک، از خدمات بهره گرفته و به شبکه متصل شود.

1-4) شبکه های بی سیم (Wi-Fi)

در هر شبکه بی سیم Access Point ها نقش سرویس دهنده و کارت های شبکه بی سـیم کـه میتوانـد بصـورت PCI، PCMCIA و USB باشند کاربران سیستم را تشکیل میدهد.

غالب تجهیزات بی سیم که برای برپایی شبکه LAN مورد استفاده قرار میگیرند مبتنی بر استاندارد 802.11 از نوع دید مستقیم هستند و گیرنده و فرستنده باید دید مستقیم به یکدیگر داشته باشند.

فاصله کاربر از Access Point، تعداد دیوارها، جنس دیوارها و نوع مصالح ساختمانی و مبلمان داخلی تاثیر گذار بر سرعت و برد شبکه دارد.

بالاترین سرعت قابل دسترس مطابق استانداردهای a802.11 و g802.11 معادل Mbps54 میباشد و سرعت های بالاتر از مکانیزم های نرم افزاری و شرایط خاص استفاده میکنند.

سرعتی که این تجهیزات مدعی آن هستند بر خلاف پیش فرض فکری بسیاری بصورت Half-Duplex است که برای مقایسه ظرفیت شبکه های بی سیم با شبکه های Ethernet باید رقم ارائه شده تجهیزات بی سیم را بر عدد دو تقسیم نمود.

در شبکه بی سیم Access Point دستگاهی است که میتوان آن را معادل هاب در شبکه Ethernet دانست و مانند هاب پهنای باند آن بصورت Shared در اختیار کاربران قرار میگیرد.

با توجه به اطلاعات بالا میتوان نتیجه گرفت که یک Access Point منطبق بر g802.11 دارای پهنای باند اشتراکی و Half-Duplex برابر Mbps54 میباشد . که میتوان گفت برابر Mbps25 بصورت Full-Duplex خواهد بود. از آنجایی که این پهنای باند اشتراکی میباشد چنانچه 5 کاربر از این Access Point بخواهند استفاده کنند هرکدام پهنای باندی برابر Mbps5 خواهند داشت مگر آنکه آنقدر خوش شانس باشند که در هر لحظه فقط یکی از این کاربران نیاز به دسترسی به منابع شبکه ای داشته باشد تا بتواند بتنهایی از Mbps25 استفاده نماید. پس محاسبه تعداد Access Pointهای مورد نیاز رابطه مستقیم با تعداد کاربران همیشه Online و میزان مصرف آنها دارد.

کاربران شبکه های بی سیم بیشترین رضایت را زمانی خواهند داشت که عمده کاربری آن جهت دسترسی به اینترنت و منابع اینترنتی باشد که برخوردای از Kbps100 هم برای کاربران کفایت خواهد کرد.

در هیچ کجا شما نمیتوانید یک خط نوشته پیدا کنید که شبکه های WLAN را جایگزینی برای شبکه هـای Ethernet معرفی کرده باشد! شبکه های WLAN یک راه حل هستند بـرای مـواقعی کـه امکـان کابـل کشـی و اسـتفاده از شـبکه Ethernet امکانپذیر نیست و یا اولویت با Mobility و یا حفظ زیبایی محیط است. سالن های کنفرانس، انبارها، محـیط های کارخانه ای، کارگاه های عمرانی و محیط هـای نمایشـگاهی بهتـرین نمونـه هـا بـرای اسـتفاده مـوثر از شـبکه هـای WLAN میباشند و اما قابل توجه دوستان امنیتی! راه اندازی یک شبکه بی سیم بسیار راحـت و سـریع امکانپـذیر اسـت ولیکن به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد. روش های مختلفی جهت امن سازی این شـبکه هـای توسعه داده شده که با صرف کمی وقت میتوان یکی از این روش ها را بکار برد تا از سوء استفاده و یا صدمه جلوگیری شود.

با توجه محدود بودن پهنای باند شبکه های بی سیم کد های مخرب مخصوصـاً کـرم هـای اینترنتـی (Worm) بسـادگی میتوانند در صورت ورود به شبکه Point Access را بدلیل بار مضاعف مختل کنند. حتماً در شبکه های بی سیم هر چند کوچک از وجود برنامه های آنتی ویروس و بروز بودن آنها اطمینان حاصل کنید. بسیار اوقات حرکـت Wormهـا باعـث از کار افتادگی Access Point و اصطلاحاً Hang کردن آن میشود که ممکن است در برداشت اولیه خراب بودن Access Point منبع مشکل تشخیص داده شود. باز یادآور میشوم شبکه های بی سیم حـداقل بـا مشخصـات فعلـی یـک راه حـل هستند برای شرایطی که در آن امکان استفاده از Ethernet و کابل کشی وجود ندارد و نه یک جایگزین Ethernet و اگر کسی غیر از این به شما گفت میتوانید بصورت خیلی خاصی (Special) در صورتش نگاهی بیاندازید! بکـارگیری از شـبکه های بی سیم در کنار شبکه Ethernet برای کاربران Mobile که ممکن است هر لحظه با Laptop و یا PDA خـود از گرد راه برسند و یا سالن کنفرانس و اجتماعات همواره بسیار سودمند و رضایت بخش خواهـد بـود. همچنـین امکـانی کـه بصورت موقتی برپا شده اند نظیر پروژه های عمرانی و نمایشگاه ها و دفاتر استیجاری نیز در فهرست مـوارد کـاربرد شـبکه های بی سیم قرار دارند. آنچه در این نوشته به آن توجه شده با این فرض صورت گرفته که هـدف از بکـارگیری تکنولـوژی Wireless جهت راه اندازی شبکه LAN بصورت بی سیم است و شامل سناریو های ارتباطـات Point-to-Point نمـی شود.در هر شبکه بی سیم Access Point ها نقش سرویس دهنده و کارت های شبکه بی سیم که میتواند بصورت PCI، PCMCIA و USB باشند کاربران سیستم را تشکیل میدهد. غالب تجهیزات بی سیم کـه بـرای برپـایی شـبکه LAN مورد استفاده قرار میگیرند مبتنی بر استاندارد 802.11 از نوع دید مستقیم هستند و گیرنده و فرستنده باید دید مستقیم به یکدیگر داشته باشند. فاصله کاربر از Access Point، تعداد دیوارها، جنس دیوارها و نوع مصالح ساختمانی و مبلمـان

داخلی تاثیر گذار بر سرعت و برد شبکه دارد. بالاترین سرعت قابل دسترس مطابق استانداردهای a802.11 و g802.11 معادل Mbps54 میباشد و سرعت های بالاتر از مکانیزم های نرم افزاری و شرایط خاص استفاده میکنند. سرعتی که این تجهیزات مدعی آن هستند بر خلاف پیش فرض فکری بسیاری بصورت Half-Duplex است که برای مقایسه ظرفیت شبکه های بی سیم با شبکه های Ethernet باید رقم ارائه شده تجهیزات بی سیم را بر عدد دو تقسیم نمود. در شبکه بی سیم Access Point دستگاهی است که میتوان آن را معادل هاب در شبکه Ethernet دانست و مانند هاب پهنای باند آن بصورت Shared در اختیار کاربران قرار میگیرد. با توجه به اطلاعات بالا میتوان نتیجه گرفت که یک Access Point منطبق بر g802.11 دارای پهنای باند اشتراکی و Half-Duplex برابر Mbps54 میباشد که میتوان گفت برابر Mbps25 بصورت Full-Duplex خواهد بود. از آنجایی که این پهنای باند اشتراکی میباشد چنانچه 5 کاربر از این Access Point بخواهند استفاده کنند هرکدام پهنای باندی برابر Mbps5 خواهند داشت مگر آنکه آنقدر خوش شانس باشند که در هر لحظه فقط یکی از این کاربران نیاز به دسترسی به منابع شبکه ای داشته باشد تا بتواند بتنهایی از Mbps25 استفاده نماید. پس محاسبه تعداد Access Pointهای مورد نیاز رابطه مستقیم با تعداد کاربران همیشه Online و میزان مصرف آنها دارد. کاربران شبکه های بی سیم بیشترین رضایت را زمانی خواهند داشت که عمده کاربری آن جهت دسترسی به اینترنت و منابع اینترنتی باشد که برخوردای از Kbps100 هم برای کاربران کفایت خواهد کرد.

در هیچ کجا شما نمیتوانید یک خط نوشته پیدا کنید که شبکه های WLAN را جایگزینی برای شبکه های Ethernet معرفی کرده باشد! شبکه های WLAN یک راه حل هستند برای مواقعی که امکان کابل کشی و استفاده از شبکه Ethernet امکانپذیر نیست و یا اولویت با Mobility و یا حفظ زیبایی محیط است. سالن های کنفرانس، انبارها، محیط های کارخانه ای، کارگاه های عمرانی و محیط های نمایشگاهی بهترین نمونه ها برای استفاده موثر از شبکه های WLAN میباشند. راه اندازی یک شبکه بی سیم بسیار راحت و سریع امکانپذیر است ولیکن به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد. روش های مختلفی جهت امن سازی این شبکه های توسعه داده شده که با صرف کمی وقت میتوان یکی از این روش ها را بکار برد تا از سوء استفاده و یا صدمه جلوگیری شود. با توجه محدود بودن پهنای باند شبکه های بی سیم کد های مخرب مخصوصاً کرم های اینترنتی (Worm) بسادگی میتوانند در صورت ورود به شبکه Access Point را بدلیل بار مضاعف مختل کنند. حتماً در شبکه های بی سیم هر چند کوچک از وجود برنامه های آنتی ویروس و بروز بودن آنها اطمینان حاصل کنید. بسیار اوقات حرکت Wormها باعث از کار افتادگی Access Point و

اصطلاحاً Hang کردن آن میشود که ممکن است در برداشت اولیه خراب بودن Access Point منبع مشکل تشخیص داده شود. باز یادآور میشوم شبکه های بی سیم حداقل با مشخصات فعلی یک راه حل هستند برای شرایطی که در آن امکان استفاده از Ethernet و کابل کشی وجود ندارد و نه یک جایگزین Ethernet و اگر کسی غیر از این به شما گفت میتوانید بصورت خیلی خاصی (Special) در صورتش نگاهی بیاندازید! بکارگیری از شبکه های بی سیم در کنار شبکه Ethernet برای کاربران Mobile که ممکن است هر لحظه با Laptop و یا PDA خود از گرد راه برسند و یا سالن کنفرانس و اجتماعات همواره بسیار سودمند و رضایت بخش خواهد بود. همچنین امکانی که بصورت موقتی برپا شده اند نظیر پروژه های عمرانی و نمایشگاه ها و دفاتر استیجاری نیز در فهرست موارد کاربرد شبکه های بی سیم قرار دارند.

فصل دوم : امنیت در شبکه های بی سیم

2-1) امنیت در شبکه های بی سیم

از آنجا که شبکه های بی سیم، در دنیای کنونی هر چه بیشتر در حال گسترش هستند و با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم به آگاهی از خطرات استفاده از این شبکه ها با وجود امکانات نهفته که در آن ها مد و پیکر بندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت. بنا داریم در این سری از مقالات با عنوان (امنیت در شبکه های بی سیم) ضمن معرفی این شبکه با تاکید بر ابعاد امنیتی آنها ، به روش های پیکر بندی صحیح که احتمال رخداد حملات را کاهش می دهد خواهیم پرداخت.

2-2) منشاء ضعف امنیتی در شبکه های بی سیم و خطرات معمول:

خطر معمول در کلیه شبکه های بی سیم مستقل از پروتکل و تکنو لوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذ گران قادرند در صورت شکستن موانع امنیتی که نچندان قدرتمند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جا زده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهندگان سازمان و مجموعه، تخریب اطلاعات ، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیر واقعی و گمراه کننده سوء استفاده از سیمهای باند موثر شبکه و دیگر فعالیتهای مخرب دارد.

2-3) شبکه های محلی بی سیم

تکنولوژی و صنعت WLAN به اوایل دهه 80 میلادی باز می گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه های محلی بی سیم به کندی صورت می پذیرد. با ارائه استاندارد IEEE 802. 11b که پهنای باند نسبتا بالایی را برای شبکه های محلی امکان پذیر می ساخت. استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاظر مقصود از WLAN تمامی پروتکل ها و استاندارد های خانوادگی IEEE 802. 11b است. این شبکه محلی بی سیم تجاری توسط Motorola پیاده سازی شد. این شبکه، به عنوان یک نمونه از این شبکه ها، هزینه ای بالا و پهنای باندی پایین را تحمیل می گردد که ابدا مقرون به صرفه نیست. از همان زمان به بعد در اوایل دهه 90 میلادی، پروژه ی استاندارد 802.11 توسط IEEE نهایی شده و تولید محصولات بسیاری برپایه ی این استاندارد ما آغاز شد . نوع a ، با استفاده از فرکانس حاصل 5GHZ ، پهنای باندی تا 5Mbps را فراهم می کند. در حالی که نوع b با استفاده از فرکانس حامل 4 GHZ و 2 ، تا 11 mbps پهنای باند را پشتیبانی می کند. با این وجود تعداد کانال های قابل استفاده در نوع bدر مقایسه با نوع a بیشتر است. تعداد این کانال ها ، با توجه به کشور مورد نظر تفاوت می کند. در حالت

معمول مقصود از WLAN استاندارد 802.11 b استاندارد دیگری نیز به تازگی توسط IEEE معرض شده است که به 802.11 g شناخته می شود. این استاندارد بر اساس فرکانس حامل 4 GHZو 2 عمل می کند ولی با استفاده از روش های نوینی می تواند پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد که مدت زیادی از نمایی شدن و معرفی آن نمی گذرد، بیش از یک سال است که آغاز شده و با توجه به سازگاری آن استاندارد 802.11 b و استفاده از آن در شبکه های بی سیم آرام آرام در حال گسترش است.

2-4) امنیت در شبکه های محلی بر اساس استاندارد 802 . 11

پس از آن که در سه قسمت قبل در مورد شبکه های بی سیم محلی و عناصر آنها پردا ختیم ،از این قسمت بررسی روشها و استاندارد های امن سازی شبکه های محلی بی سیم مبتنی بر استاندارد IEEE 802 .11 را آ غاز می کنیم . با طرح قا بلیت های امنیتی این استاندارد ،می توان از محدو دیت های آن آگاه شد و این استاندارد و کار برد را برای موارد خاص و مناسب مورد استفاده قرار داد .

استاندارد 11و 802 سرویس های جدا و مشخصی را برای تا مین یک محیط امن بی سیم در اختیار قرار می دهد . این سر ویس ها اغلب توسط پروتکل (WEP (wired Equivalent privacy تامین می گردند و وظیفه آنها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است . درک لایه یی که این پروتکل به امن سازی آن می پردازد اهمیت ویژ ه ای دارد ،به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر ، غیر از لایه ارتباطی بی سیم که مبتنی بر استاندارد 11 و 802 است ، کاری ندارد .این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درو نی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست .زیرا امکان

قصور از دیگر اصول امنیتی در سطوح بالا تر ارتباطی وجود دارد .در حال حاضر عملا تنها پروتکلی که امنیت اطلا عات و ار تبا طات را در شبکه های بی سیم بر اسا س استاندارد 11 و 802 فرا هم می کند WEP است

این پروتکل با وجود قابلیت هایی که دارد ،نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی ، ولو سخت و پیچیده فرا هم می کند . نکته یی که باید به خاطر داشت این است که حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم ، ریشه در پیکر بندی نا صحیح WEP در شبکه دارد . به عبارت دیگر این پروتکل در صورت پیکر بندی صحیح در صد بالا یی از حملات را نا کام می گذارد ،هر چند که فی نفسه دچار نواقص و ایراد هایی نیز هست .بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی به شبکه ی سیمی دارای اشتراک هستند . به عبارت دیگر نفوذ گران بعضا با استفاده از راه های ارتبا طی دیگری که بر روی مخدوم ها و سخت افزار های بی سیم ،خصوصا مخدوم های بی سیم ، وجود دارد به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هر چند جزئی میان امنیت در شبکه های سیمی و بی سیمی است که از نظر ساختاری و فیزیکی با یک دی گر اشتراک دارند .

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد :

1) Authentication

هدف اصلی WEP ایجاد مکانی برای احراز هویت مخدوم بی سیم است .این عمل که در واقع کنترل دسترسی به شبکه ی بی سیم است .این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد .

2) Confidentiality

محرمانه گی هدف دیگر WEP است . این بعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است . سیاست این بخش از WEP از سرقت اطلا عات در حال انتقال بر روی شبکه ی محلی بی سیم است

3) Integrity

هدف سوم از سر ویس ها و قابلیت های WEP طراحی سیاستی است که تضمین می کند پیامها و اطلاعات در حال تبا دل در ، شبکه خصو صا میان مخدوم های بی سیم و نقاط دسترسی ، در حین انتقال دچار تغییر نمی گردند . این قابلیت در تمامی

استاندارد ها ، بستر ها و شبکه های ار تباطی دیگر نیز کم و بیش وجود دارد . نکته ی مهمی در مورد سه سرویس WEP وجود دارد نبود سر ویس های وصول Auditing و Authorization در میان سرویس های ارایه شده توسط این پروتکل است .

5-2) سرویس های امنیتی WEP _ Authentication :

در قسمت قبلی به معرفی پروتکل WEP که عملا تنها روش امن سازی ارتباطات در شبکه های بی سیم بر مبنای استاندارد 11و 802 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم در این قسمت به معرفی سرویس های اول یعنی Authentication میپردازیم

1) Authentication

استاندارد 11و802 دو روش برای احراز هویت کاربرانی که در خواست اتصال به شبکه های بی سیم را به نقاط دسترسی ارسال میکنند ، دارد که یک روش بر مبنای روز نگاری ست و دیگری از روز نگاری استفاده نمی کنند .

2) Authentication بدون روز نگاری :

در روشی که مبتنی بر روزنگاری نیست ، دو روش برای تشخیص هویت مخدوم وجود دارد . در هر روش مخدوم متقاضی پیوستن به شبکه ،در خواست ارسال هویت از سوی نقطه ی دسترسی را با پیامی حاوی یک SSID (service set Identifier) پاسخ می دهد در روش اول که Authentication open system موسوم است یک SSID خالی نیز برای دریافت اجازه اتصال به شبکه کفایت می کند در واقع در این روش تمامی مخدوم هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می کنند با پاسخ مثبت روبه رو می شوند و تنها آدرس آنها توسط نقطه های دسترسی نگه داری می شود به همین دلیل به این روش Authentication Null نیز اطلاق می شود در بخش دوم از این نوع ، باز هم یک SSID به نقطه ی دسترسی ارسال میگردد . با این تفاوت که اجازه ی اتصال به شبکه تنها در صورتی از سوی نقطه ی دسترسی صادر می گردد که SSID ی ارسال شده جزو SSID های مجاز برای دسترسی به شبکه باشند . با این روش به Closed Authentication system موسوم است .

نکته ای که در این میان اهمیت بسیاری دارد توجه به سطح امنیتی ست که این روش در اختیار ما می گذارد این دو روش عملا روش امنی از احراز هویت را ارئه نمیدهد و عملا تنها راه برای آگاهی نسبتی و نه قطعی از هویت در خواست کننده هستند با این وصف از آن جایی که امنیت در این حالات تضمین شده نیست و معمولا حملات موفق بسیاری ، حتی توسط نفوذ گران کم تجربه و مبتدی ، به شبکه هایی که بر اساس این روش ها عمل میکنند رخ میدهد . لذا این دو روش در حالتی کاربرد دارند که یا شبکه در حال ایجاد است که حاوی اطلاعات حیاتی نیست ، یا احتمال رخداد حمله را به آن بسیار کم است . هر چند که با توجه پوشش نسبتا گسترده ی یک شبکه های بی سیم – که مانند شبکه های بی سیمی امکان محدود سازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد !

6-2) Authentication با روز نگا ری 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 تایید می شود . در این روش ، نقطه دسترسی (AP) یک رشته ی تصادفی تولی کرده و ان را به مخدوم میفرستد . مخدوم این رشته ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده میشود) روز میکند و حاصل را برای نقطه ی دسترسی ارسال می کند نقطه ی دسترسی به روش معکوس پیام دریافتی را روز گشایی کرده و با رشته ی ارسال شده مقایسه می کند دو صورت هم رسانی این دو پیام ، نقطه ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل میکند روش روز نگاری و روز گشایی در این تبادل روش RC4 است در این میان با فرض اینکه روز نگاری RC4 را روشی کاملا مطمئن بدانیم ، دو خطر کمین این روش است :

الف) در این روش تنها نقطه ی دسترسی ست که از هویت مخدوم اطمینان حاصل می کند به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه ی دسترسی که ان را با حال تبادل داده هایی روزی ست نقطه دسترسی اصلی است .

ب) تمامی روش هایی که مانند این روش بر پایه ی سوال و جواب بین دو طرف ، با هدف احراز هویت یا تبادل اطلاعات حیاتی ، قرار دارند با جملاتی تحت عنوان man- in –the middle در خطر هستند در این دسته از حملات نفوذ گر میان دو طرف قرار می گیرد و به گونه یی هر یک از دو طرف را گمراه می کند .

2-7) سرویس های امنیتی Integrity, 802,11b – privacy

در قسمت قبل به سرویس اول از سرویس های امنیتی 802, 11b پرداختیم این قسمت به بررسی دو سرویس دیگر اختصاص دارد سرویس اول privacy (محرمانه گی) و سرویس دوم integrity است

❖ **Privacy** :

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان con fidentiality ازآن یاد می گردد به معنای حفظ امنیت و محرمانه نگه داشتن اطلاعات کاربر یا گروه های در حال تبادل اطلاعات با یکدیگر است . برای رعایت محرمانگی عموما از تکنیک های روزنگاری استفاده می گردد به گونه یی که در صورت شنود اطلاعات در حال تبادل ، این اطلاعات بدون داشتن کلید های رمز ، قابل رمز گشایی نبوده و لذا برای شنود گر غیر قابل سوء استفاده است در استاندارد 802,11b از تکنیک های رمز نگاری WEP استفاده می گردد که بر پایه ی RC4 است RC4 یک الگوریتم رمز نگاری متقارن است که در آن یک رشته ی نیمه تصادفی تولید می گردد و توسط آن کل داده رمز می شود این رمز نگاری بر روی تمام بسته ی اطلاعات پیاده می شود به بیان دیگر داده های تمامی لایه های بالایی اتصال بی سیم نیز توسط این روش رمز می گردند از IP گرفته تا لایه های بالاتری مانند HTTP از آنجایی که این روش عملا اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه ها ی محلی بی سیم مبتنی بر استاندارد 802,11b است معمولا به کل پروسه ی امن سازی اطلاعات در این استاندارد به اختصار WEP گفته می شود کلید های WEP اندازه های از 40 بیت تا 140 بیت می توانند داشته باشند این کلید ها با IV (مختلف Initiali zatiavector یا بردار اولیه) 24 بیتی ترکیب شده و یک کلید 128 بیتی RC4 را تشکیل میدهند طبیعتا هر چه اندازه ی کلید بزرگ تر باشد امنیت اطلاعات بالاتر است . تحقیقات نشان می دهد که استفاده از کلید هایی با اندازه 80 بیت یا بالاتر عملا استفاده از تکنیک brute-force را بریا شکستن رمز غیر ممکن می کند به عبارت دیگر تعداد کلید های ممکن برای اندازه یی بالاست که قدرت پردازش

سیستم های رایانه یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی کند . هرچند که در حال حاضر اکثر شبکه ها ی محلی بی سیم از کلید های 40 بیتی برای رمز کردن بسته های اطلاعاتی استفاده می کنند ولی نکته ییکه اخیرا بر اساس یک سری آزمایشات به دست آمده است ، این است که روش تامین محرمانگی توسط WEP در مقابل حملات دیگری ، غیر از استفاده از روش brute- force نیز آسیب پذیر است این آسیب پذیری ارتباطی به اندازه ی کلید استفاده شده ندارد .

❖ **Integritg** :

مقصود از Integritg صحت اطلاعات در حین تبادل است وسیاست های امنیتی یی که Integritg را تضمین می کنند روش هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم ترین میزان تقلیل میدهند .

در استاندارد 802,11b نیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در حال تبدیل میان مخدوم های بی سیم و نقاط دسترسی کم میشود روش مورد نظر استفاده از یک کد CRC است همان طور که در شکل مقابل نیز نشان داده شده است ، یک CRC-32 قبل از رمز بسته تولید می شود در سمت گیرنده ، پس از رمز گشایی ، CRC داده های رمز گشایی شده مجددا محاسبه شده و با CRC نوشته شده در بسته مقایسه می گردد که هر گونه اختلاف میان دو CRC به معنای تغییر محتویات بسته است در حین تبادل است . متا سفانه این روش نیز مانند رمز نگاری توسط RC4 ، مستقل از اندازه ی کلید امنیتی مورد استفاده ، در مقابل برخی از حملات شناخته شده آسیب پذیر است .

متاسفانه استاندارد 802,11b هیچ مکانیزمی برای مدیریت کلید های امنیتی ندارد و عملا تمامی عملیاتی که برای حفظ امنیت کلید ها انجام می گردد و باید توسط کسانی که شبکه های بی سیم را نصب می کنند به صورت دستی پیاده سازی گردد از انجایی که این بخش از امنیت یکی از معضل های اساسی در مبحث رمز نگاری است ، با این ضعف عملا روش های متعددی برای حمله به شبکه های بی سیم قابل تصور است

این روش ها معمولا برسهل انگاری های انجام شده از سوی کاربران و.مدیران شبکه مانند تغییر ندادن کلید به صورت مداوم ، لو دادن کلید ، استفاده از کلید های تکراری یا کلید های پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یجز درصد نسبتا بالایی از حملات موفق به شبکه های بی سیم ندارد این مشکل از شبکه ها ی بزرگ تر بیش تر خود را نشان می دهد حتی با فرض تلاش برای جلوگیری از رخ دادن چنین سهل انگاری هایی زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملا کنترل کردن این تعداد بالا بسیار دشوار شده و گه گاه خطا هایی در گوشه و کنار این شبکه ی نسبتا بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود .

2-8) ضعف های اولیه امنیتی WEP

در قسمت قبل به سرویس های امنیتی استاندارد 11و802 پرداختیم در ضمن ذکر هریک از سرویس ها ، سعی کردیم به ضعف های هریک اشاره داشته باشیم در این قسمت به بررسی ضعف های تکنیک های امنیتی پایه ی استفاده شده در این استاندارد می پردازیم . همان گونه که گفته شد عملا پایه ی امنیت در استاندارد 11و802 براساس پروتکل WEP استوار است WEP در حالت استاندارد بر اساس کلید های 40 بیتی برای رمز نگاری توسط الگوریتم RC4 استفاده می شود هر چند که برخی از تولیدکنندگان نگارش های خاصی از WEP را با کلید هایی با تعداد بیت های بیش ترپیاده سازی کرده اند نکته یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالا رفتن امنیت WEP اندازه ی کلید هاست . با وجود ان که با بالا رفتن اندازه کلید (تا 104 بیت) امنیت بالاتر میرود ولی از آن جا که این کلید ها توسط کاربران WEP بر اساس یک کلمه عبور تعیین می شود تضمینی نیست که این اندازه تماما استفاده شود از سوی دیگر همان طور که در قسمت های پیشین نیز ذکر شد دست یابی به این کلید ها فرایند چندان سختی نیست ، که در آن صورت دیگر اندازه ی کلید اهمیتی ندارد . مختصات امنیت بررسی های بسیاری را برای

تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع ، شامل حملات غیر فعال وفعال است تحلیل شده است .

حاصل برسی انجام شده فهرستی از ضعف های اولیه ی این پروتکل است :

2-9) استفاده از کلید های ثابت WEP

یکی از ابتدایی ترین ضعف ها که عموما در بسیاری از شبکه ها ی محلی بی سیم WEP وجود دارد استفاده کلید های مشابه توسط کاربران برای مدت زمان نسبتا زیاد است این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده میکند به سرقت برود یا برای مدت زمانی در دسترس نفوذ گر باشد کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه هایی کاری عملا استفاده از تمامی این ایستگاه ها نا امن است.

از سوی دیگر با توجه به مشابه بودن کلید در هر لحظه کانال ارتباطی زیادی توسط یک حمله نفوذ پذیر هستند این بردار که یک فیلد 24 بیتی است در قسمت قبل معرفی شده است .

این بردار به صورت متنی ساده فرستاده می شود از آن جایی که کلید ی که برای رمز نگاری مورد استفاده قرار می گیرد براساس IV تولید می شود محدودهی IV عملا نشان دهنده ی احتمال تکرارآن ودر نتیجه احتمال تولید کلید های مشابه است به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می توان به کلید های مشابه دست یافت این ضعف در شبکه ها ی شلوغ به مشکلی حاد مبدل می شود خصوصا اگر از کارت شبکه ی استفاده شده مطمئن نباشیم بسیاری از کارت های شبکه ازIV های ثابت استفاده میکنند وبسیاری از کارت های شبکه ی یک تولید کنندهی واحد IV های مشابه دارند . این خطر به همراه ترافیک بالا در یک شبکه ی شلوغ احتمال تکرار IV در مدت زمان کوتاه رابالاتر می برد WEP

در نتیجه کافی ست نفوذ گر در مدت زمانی معین به ثبت داده های رمز شده ی شبکه بپردازد وIV های پسته های اطلاعاتی را ذخیره کند با ایجاد بانکی ازIV های استفاده شده در یک شبکه ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت .

2-10) ضعف در الگوریتم

از ان جایی کهIV در تمامی بسته های تکرار می شود WEP بر اساس آن کلیدی تولید می شود ، نفوذ گر می تواند با تحلیل وآنا لیز تعداد نسبتا زیادی از IV ها وبسته های رمز شده وبر اساس کلید تولید شده بر مبنای آنIV ، به کلید اصلی دست پیدا کند این فرایند عملی زمان بر است ولی از انجا که اتصال موفقیت در ان وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می گردد

2-11) استفاده از CRC رمز نشده :

در پروتکل WEP ، کدCRC رمز نمی شود . لذا بسته های تاییدی که این از سوی نقاط دسترسی بی سیم به سوی گیرنده ارسال می شود براساس یک CRC رمز نشده ارسال می گردد WEP تنها در صورتی که نقطه دسترسی از صحت بسته اطمینان حاصل کند تایید آن را می فرستد . این ضعف این امکان را فراهم میکند که نفوذ گر برای رمز گشایی یک بسته ، محتوای آن را تغییر دهد وCRC را نیز به دلیل این که رمز نشده است به راحتی عوض کندومنتظر عکس العمل نقطه ی دسترسی بماند که این آیا بسته تایید را صادر می کند یا خیر ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هعستند نکته یی که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آنها (مشکل امنیتی سوم) به ضعف در الگوریتم رمز نگاری بازمی گردد ولذا با تغییر الگوریتم رمز نگاری تنها این ضعف است که برطرف می گردد وبقیه ی مشکلات امنیتی کما

کان به قوت خود باقی هستند . در قسمت های آتی به برسی خطرهـای ناشـی از ایـن ضـعف هـا ونیازهـای امنیتی در شبکه بی سیم می پردازیم .

12-2) خطر ها ، حملات امنیتی

همان گونه که گفته شد ، با توجه به پیشرفت های اخیر ، در آینده یی نه چندان دور باید منتظـر گسـترده گی هر چه بیش تر استفاده از شبکه های بی سیم باشیم این گسترده گی با توجه بـه مشـکلاتی کـه ازنظـر 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 وشرکت های بزرگ است ، توسعه ی ایـن اسـتاندارد را در ابهام فروبرده است .و دراین قسمت به دسته بندی WEP تعریف حملات ، خطرها WEP ریسک هـای موجود در استفاده از شبکه ها ی محلی بی سیم بر اساس استاندارد IEEE.802,11x میپردازیم حملات امنیتی به دو دسته فعال وغیر فعال تقسیم می گردند .

- حملات غیر فعال :

در این قبیل حملات نفوذ گر تنها به منبعی از اطلاعات به نحوی دست می یابدولی اقدام به تغییر محتـوای اطلاعات منبع نمیکند این نوع حمله میتواند تنها به یکی از اشکال شنود ساده یا آنا لیز ترافیک باشد .

- شنود :

در این نوع ، نفوذ گر تنها به پایش اطلاعات رد وبدل شده می پردازد برای مثال شنود ترافیـک روی یـک شبکه ی محلی بی سیم(که مد نظر ماست) نمونه هایی از این نوع حمله به شمار می آیند .

- آنا لیز ترافیک :

در این نوع حمله ، نفوذ گر با کپی برداشتن از اطلاعات پاپش شده به تحلیل جمعی داده هـا مـی پـردازد به عبارت دیگر بسته یا بسته های اطلاعات به همراه یکدیگر اطلاعات معنا داری را ایجاد می کنند .

- حملات فعال :

در این نوع حملات ، بر خلاف حملات غیر فعال ، نفوذ گر اطلاعات مورد نظر را که از منابع بـه دسـت مـی آید ، تغییر میدهد که تبعا انجام این تغییرات مجاز نیست از ان جای که در این نوع حملات اطلاعات تغییر می کنند شناسایی رخ داده حملات فرایندی امکان پذیر است . در این حملات به چهار دسته مرسـوم زیـر تقسیم بندی می گردند :

- تغییر هویت

در این نوع حمله ، نفوذ گر هویت اصلی را جعل می کند . این روش شامل تغییر هویت اصلی یکی از طـرف های ارتباط با قلب هویت ویا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد .

- پاسخ های جعلی :

نفوذ گر در این قسم از حملات بسته های که طرف گیرنده اطلاعات رد یـک ارتبـاط در یافـت مـی کنـد را پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال میگردند این نوع حمله بیش تر در موردی کاربر دارد که فرستنده اقدام به تعیـین هویـت گیرنـده مـی کنـد در ایـن حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سوالات فرستنده ارسال می گردند به معنای پر چمی برای شناسایی گیرنده محسوب میگردند ، لذا در صورتی که نفوذ گر این بسـته هـا را ذخیـره کنـد ودر زمانی که یا گیرنده فعال نیست . یا فعالیت یا ارتباط آن به صورت آگاهانه به روشـنی توسـط نفـوذ گـر قطع شده است ، میتواند مورد استفاده قرار گیرد . نفوذ گر با ارسال مجدد این بسـته هـا خـود را بـه جـای گیرنده جا زده واز سطح دسترسی مورد نیاز برخودار می گردد .

فصل سوم : ده نکته اساسی در امنیت شبکه های WI-FI

ده نکته اساسی در امنیت شبکه های WI-FI

۱ – کلمه عبور پیش‌فرض سرپرست را تغییر دهید

در هسته بیشتر شبکه‌های وای‌فای خانگی، یک روتر یا اکسس پوینت قرار گرفته است. برای راه‌اندازی این تجهیزات، تولیدکنندگان صفحات وبی را تأمین می‌کنند که به کاربر امکان می‌دهند آدرس شبکه و اطلاعات حساب کاربری خود را وارد کنند. این ابزارهای وب با یک صفحه Login (با نام کاربری و کلمه عبور) محافظت می‌شوند تا فقط دارندگان قانونی این اطلاعات بتوانند به این تنظیمات دسترسی داشته باشند. با این‌حال، اطلاعات Login پیش‌فرض بیشتر تجهیزات شبکه‌سازی بسیار ساده بوده و هکرهای اینترنتی کاملاً از آن‌ها آگاهی دارند. بنابراین، بهتر است به محض راه‌اندازی شبکه خود، این تنظیمات را تغییر دهید.

۲ – رمزگذاری WPA/WEP را فعال کنید

تمام تجهیزات وای‌فای از قالب‌های مختلف رمزنگاری پشتیبانی می‌کنند. فناوری رمزنگاری، پیام‌های ارسال شده روی شبکه‌های بی‌سیم را طوری درهم می‌ریزد که به آسانی قابل دسترس نباشند. امروزه، فناوری‌های مختلفی برای رمزنگاری ارائه شده‌اند. به‌طور طبیعی شما می‌خواهید قوی‌ترین فرم رمزنگاری را انتخاب کنید که با شبکه بی‌سیم شما کار می‌کند. با این‌حال، براساس نحوه کار این فناوری‌ها، تمام ابزارهای وای‌فای روی شبکه شما باید از تنظیمات رمزنگاری یکسانی استفاده کنند. بنابراین، شما باید یک «کوچک‌ترین مخرج مشترک» را به‌عنوان گزینه مورد استفاده خود پیدا کنید.

۳ – SSID پیش‌فرض را تغییر دهید

تمام روترها و اکسس‌پوینت‌ها از یک نام شبکه استفاده می‌کنند که تحت عنوان SSID شناخته می‌شود. تولیدکنندگان معمولاً محصولات خود را با مجموعه SSID مشابهی ارائه می‌کنند. به عنوان مثال، SSID ابزارهای Linksys معمولاً «linksys» است. البته، آگاهی از SSID به همسایگان شما اجازه نمی‌دهد که به شبکه‌تان نفوذ کنند، اما این نخستین‌قدم در مسیر هک یک شبکه است. مهم‌تر این‌که وقتی هکر بتواند یک SSID پیش‌فرض را پیدا کند، متوجه می‌شود که شبکه مورد نظر از پیکربندی ضعیفی برخوردار است و به همین دلیل، انگیزه بیشتری برای حمله به آن خواهد داشت. در هنگام پیکربندی امنیت بی‌سیم روی شبکه خودتان، بلافاصله SSID پیش‌فرض را تغییر دهید.

۴ – فیلترگذاری آدرس MAC را فعال کنید

هر یک از تجهیزات وای‌فای یک شناسه منحصربه‌فرد را ارائه می‌کند که تحت عنوان آدرس فیزیکی یا آدرس MAC شناخته می‌شود. روترها و اکسس‌پوینت‌ها رد آدرس‌های MAC تمام ابزارهایی را که به آن‌ها متصل شده‌اند، حفظ می‌کنند. بسیاری از این محصولات، گزینه‌ای را در اختیار کاربر قرار می‌دهند تا آدرس‌های MAC تجهیزات خانگی خود را وارد کرده و اتصالات شبکه را تنها با این ابزارها برقرار کنند. حتماً از این ویژگی استفاده کنید، اما باید بدانید آن‌قدرها که به نظر می‌رسد قدرتمند نیست. هکرها و برنامه‌های مورد استفاده آن‌ها به آسانی می‌توانند آدرس‌های MAC را جعل کنند.

۵ – SSID Broadcast را غیرفعال کنید

در شبکه‌سازی وای‌فای، روتر یا نقطه دسترسی بی‌سیم معمولاً نام شبکه (SSID) را در فاصله‌های زمانی معینی Broadcast می‌کند. این ویژگی برای Hotspotهای موبایل و شرکت‌هایی طراحی شده بود که در آن‌ها امکان داشت کلاینت‌های وای‌فای به دفعات از برد شبکه خارج و دوباره به آن وارد شوند. با این‌حال، ویژگی مذکور در یک خانه غیرضروری است و از سوی دیگر احتمال نفوذ بیگانگان به شبکه شما را نیز افزایش می‌دهد. خوشبختانه بیشتر نقاط دسترسی وای‌فای به سرپرست شبکه اجازه می‌دهند که ویژگی SSID Broadcast را غیرفعال کند.

۶ – به‌طور خودکار به شبکه‌های وای‌فای باز متصل نشوید

اتصال به یک شبکه وای‌فای باز مانند یک Hotspot بی‌سیم رایگان یا روتر همسایه‌تان می‌تواند کامپیوتر شما را در معرض ریسک‌های امنیتی قرار دهد. با وجود آن‌که این ویژگی معمولاً فعال نیست، اما بیشتر کامپیوترها دارای تنظیماتی هستند که امکان برقراری خودکار این نوع اتصالات را (بدون آگاه کردن شما) فراهم می‌کند. این تنظیمات به استثنای شرایط موقتی نباید فعال باشند.

۷ – به ابزارهای خود آدرس‌های IP ثابت اختصاص دهید

بیشتر شبکه‌سازهای خانگی به سمت استفاده از آدرس‌های IP داینامیک گرایش دارند. راه‌اندازی فناوری DHCP فوق‌العاده آسان است. متأسفانه این راحتی در عین حال شامل مهاجمان شبکه نیز می‌شود و به آن‌ها امکان می‌دهد که به‌آسانی آدرس‌های IP معتبری را از مجموعه DHCP شبکه شما به‌دست آورند. ویژگی DHCP را روی روتر یا نقطه‌دسترسی خود غیرفعال کرده و در مقابل یک دامنه ثابت از آدرس‌های IP را مشخص کنید. در مرحله بعد، هر یک از ابزارهای متصل به شبکه خود را برای انطباق با این دامنه پیکربندی

کنید. برای جلوگیری از دسترسی مستقیم از اینترنت به کامپیوترهای خود، می‌توانید از یک دامنه آدرس IP خصوصی (مانند x۱۰,۰,۰,) استفاده کنید.

۸ – فایروال‌ها را روی هر کامپیوتر و روتر فعال کنید

روترهای مدرن شبکه از قابلیت فایروال توکار برخوردارند، اما گزینه‌ای برای غیرفعال کردن این قابلیت نیز وجود دارد. مطمئن شوید که فایروال روتر شما فعال است برای محافظت بیشتر، نصب و اجرای یک نرم‌افزار فایروال شخصی روی هر کامپیوتر متصل به روتر را جدی بگیرید.

۹ – روتر یا اکسس پوینت را در محل امنی قرار دهید

سیگنال‌های وای‌فای معمولاً به خارج از محیط یک خانه می‌رسند. مقدار کمی نشت سیگنال از یک شبکه وای‌فای چندان مهم نیست، اما هر چه این سیگنال به مسافت دورتری برسد، تشخیص و بهره‌برداری از آن برای دیگران آسان‌تر خواهد بود. در هنگام نصب یک شبکه خانگی بی‌سیم، موقعیت روتر یا نقطه‌دسترسی است که برد آن را مشخص می‌کند. برای آن‌که نشت سیگنال به حداقل برسد، سعی کنید این ابزارها را در نقطه مرکزی خانه خود قرار دهید نه نزدیک پنجره‌ها.

۱۰- اگر برای مدت زیادی از شبکه استفاده نمی‌کنید، آن را خاموش کنید

نقطه نهایی در معیارهای امنیتی بی‌سیم، خاموش کردن شبکه‌تان برای قطع کامل دسترسی هکرها به آن است. البته، خاموش نگه‌داشتن یک شبکه به‌طور مداوم کاملاً غیرعملی است، اما می‌توانید در مواقعی که به مسافرت می‌روید یا به هر دلیل برای مدت طولانی از شبکه خود استفاده نمی‌کنید، آن را خاموش کنید.

نتیجه گیری

یک موضوع مشترک مسائل امنیت این است که مکانیسم های تکنولوژیکی برای بسیاری از رخنه های مشاهده شده وجود دارد و به خوبی درک می شوند، اما باید به منظور محافظت از شبکه فعال شوند. اقدامات پیشگیرانه معقول می توانند شبکه های بی سیم را برای هر سازمانی که می خواهد فوائد سیار بودن و انعطاف پذیری را در کنار هم گرد آورد، امن کنند. همراه با به کارگیری بسیاری از تکنولوژی های شبکه، ایده اصلی و کلیدی، طراحی شبکه با در نظر داشتن امنیت در ذهن است. بعلاوه انجام نظارت های منظم را برای تضمین اینکه طراحی انجام شده اساس پیاده سازی است، باید در نظر داشت. یک آنالایزر شبکه بی سیم یک ابزار ضروری برای یک مهندس شبکه بی سیم است.

منابع :

- ✓ سایت مجله شبکه های کامپیوتری (www.shabakeh-mag.com)
- ✓ سایت تکفا (سازمان نظام صنفی رایانه ای کشور)(www.irannsr.org)
- ✓ Http: //www. freesof.org /cIE/ topics /57
- ✓ http://www. Dei.isep.ipp.pt/docs /arpa.html
- ✓ Http://www.microsoft.com/wifi
- ✓ www.hajarian.com/mehre-alborz/salimi.pdf
- ✓ Http: //www.IEEE.org
- ✓ http://www. Dei.isep.ipp.pt/docs /arpa.html
- ✓ www.iran24h.com/more/m000923.doc