www.takbook.com

باسمه تعالی

عنوان:

امنیت در شبکه های وای فای
(Wi-Fi Security)

گردآورنده:

جواد حاجیان نژاد

www.takbook.com

www.takbook.com

بسم الله الرحمن الرحیم

www.takbook.com

www.takbook.com

تقدیم به مادر بزرگوارم که هرچه دارم از اوست....

www.takbook.com

www.takbook.com

چکیده

امروزه امنیت یکی از ضروری ترین مواردی است که در راه اندازی هر شبکه ای باید اعمال گرد. با گسترش شبکه های بی سیم (وای فای) و استفاده زیاد و عمومی شدن این شبکه ها،برقراری امنیت درآن یک امر مهم و ضروری می باشد. همانطور که راه اندازی این شبکه بی سیم بسیار راحت و اتصال به آن نیز بسیار سریع می باشد، به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد.امنیت در شبکه های وای فای که در کاربردهای نظامی،تجاری و سازمانی هستند به یکی از بزرگترین چالش های این شبکه ها تبدیل شده است و نشت هرگونه اطلاعات یا آسیب رسیدن به شبکه می تواند فاجعه انگیز باشد وگاها جبران آن غیر ممکن باشد.

با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به مدد پیکربندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت.

در این مجموعه سعی کرده ام که معرفی اجمالی از طریقه کار این شبکه ها و استاندارد ها و پروتکل های به کار رفته در آن بپردازم،سپس به معرفی مفاهیم و چالش های امنیتی موجود و راه حل آنها و در نهایت ارائه پروتکل ها و استاندارد های امنیتی در این شبکه ها بپردازم.

جواد حاجیان نژاد- مشهد مقدس

www.takbook.com

www.takbook.com

فهرست مطالب

فصل اول : معرفی شبکه های وای فای ۹

۱-۱ شبکه های Wi-Fiچیست؟ ۱۰
۱-۲ کاربردهایWi-Fi ۱۱
۱-۳ دلایل رشد Wi-Fi ۱۲
۱-٤ ترکیب سیستم Wi-Fi با رایانه ۱٤
۱-۵ شبکه Wi-Fi چگونه کار می کنند؟ ۱٤
۱-٦ تحلیل ترافیک شبکه های Wi-Fi ۱۵
۱-۷ آینده شبکه های Wi-Fi ۱۸
۱-۸ نتیجه گیری ۱۸

فصل دوم : استاندارد های شبکه محلی بی سیم ۱۹

۲-۱ معرفی ۲۰
۲-۲ معماری شبکه های محلی بی سیم ۲۳
۲-۲-۱ همبندی های ۸۰۲.۱۱ ..... ۲۳
۲-۳ خدمات ایستگاهی ۲۵
۲-٤ خدمات توزیع ۲٦
۲-۵ دسترسی به رسانه ۲۷
۲-۵- الایه فیزیکی ۲۸
۲-٦ استاندارد 802.11B ۳۵
۲-٦-۱اثرات فاصله ۳٦
۲-٦-۲پل بین شبکه ای ۳٦
۲-۷ استاندارد 802.11A ۳۷
۲-۸ استاندارد بعدی IEEE 802.11G ۳۹

فصل سوم :مفاهیم امنیتی در شبکه های بی سیم ٤۰

۳-۱ فاکتور های امنیتی در شبکه های بی سیم ٤۱
۳-۲ سیستم تشخیص نفوذ ٤۳
۳-۳ چالش های امنیتی در شبکه های WI-Fi ٤٦
۳-٤ نقاط آسیب پذیر و قابل نفوذ در شبکه های Wi-Fi ٤۷
۳-۵ امن سازی شبکه های بی سیم ۵۰
۳-۵-۱احراز هویت ۵۰
۳-۵-۲امنیت داده ها ۵۳

www.takbook.com

www.takbook.com

۳-۶ مدیریت کلید ها ۵۴
۳-۷ صحت داده ۵۵
۳-۸ نتیجه گیری ۵۵

فصل چهارم :چالش های امنیتی و راه کار ها در شبکه های وای فای ۵۶

۴-۱ مقدمه ۵۷
۴-۲ مشکل اول: دسترسی آسان ۵۷
۴-۲-۱ راه حل مشکل اول: تقویت کنترل دسترسی قوی ۵۸
۴-۳ مسأله دوم: نقاط دسترسی نامطلوب ۵۹
۴-۳-۱ راه حل مشکل دوم : رسیدگی های منظم به سایت ۶۰
۴-۴ مشکل سوم استفاده غیرمجاز از سرویس ۶۱
۴-۴-۱ راه حل مشکل سوم : طراحی و نظارت برای تأیید هویت محکم ۶۲
۴-۵ مشکل چهارم : محدودیت های سرویس و کارایی ۶۲
۴-۵-۱راه حل مشکل چهارم : دیدبانی شبکه ۶۳
۴-۶ مشکل پنجم جعل MAC و SESSION ربایی! ۶۴
۴-۶-۱ راه حل شماره۵ : پذیرش پروتکل های قوی و استفاده از آنها ۶۵
۴-۷ مشکل ششم: تحلیل ترافیک و استراق سمع ۶۵
۴-۷-۱ راه مشکل ششم : انجام تحلیل خطر ۶۶
۴-۸ مشکل هفتم: حملات سطح بالاتر ۶۷
۴-۸-۱راه حل مشکل هفتم : هسته را از LAN بی سیم محافظت کنید ۶۷
۴-۹ چند نکته در مورد امن سازی شبکه های وای فای ۶۷
۴-۱۱ جمع‌بندی ۷۹

فصل پنجم:پروتکل های امنیتی در شبکه های وای فای ۸۱

۵-۱ مقدمه ۸۲
۵-۲ پروتکل اتصال/دسترسی در شبکه های وای فای ۸۲
۵-۳ قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱ ..... ۸۳
احراز هویت(Authentication) ۸۴
محرمانگی (Confidentiality) ۸۴
صحت(Integrity) ۸۵
۵-۴ خدمات ایستگاهی ۸۵
۵-۴-۱ احراز هویت Authentication ۸۶
۵-۴-۲ سرویس امنیت (Privacy یا confidentiality) ۸۶
۵-۴- ۳صحت (Integrity) ۸۸
۵-۵ ضعف‌های اولیه‌ی امنیتی WEP ۸۹

www.takbook.com

www.takbook.com

۵-۵-۱ استفاده از کلیدهای ثابت WEP ۹۰
۵-۵-۲ Initialization Vector – IV ۹۰
۵-۵-۳ ضعف در الگوریتم ۹۰
۵-۵-٤استفاده از CRC رمز نشده ۹۱
۵-٦ پروتکل WPA(Wi-Fi Protected Access) ۹٤
۵-۷ پروتکل WPA2 ..... ۹٦
۵-۸ پروتکل امنیتی WPS ۹۸
۵-۹ جمع بندی ۹۹
مشکلات فعلی و کارهای آتی ۱۰۰

www.takbook.com

www.takbook.com

مقدمه

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.

شبکه های WLAN را نمی توان جایگزینی برای شبکه های Ethernet معرفی کرده ،بلکه 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.

شبکه های LAN به صورت ذاتی از شبکه های بی سیم امن تر می باشند، چرا که از نظر ساختاری قسمت عمده و یا تمام ساختار آنها در درون یک ساختمان قرار دارد و بدین دلیل از دسترسی های غیر مجاز در امان هستند. اما شبکه های بی سیم که با استفاده از امواج رادیویی فعالیت می کنند از آنجا که همانند شبکه های LANدارای ساختاری فیزیکی نیستند، بیشتر در معرض نفوذ قرار داشته و آسیب پذیرترند،بنابراین مسئله امنیت به طور جدی در این شبکه ها مطرح می شود و گاها مسائل و مشکلاتی امنیتی که در این شبکه ها وجود دارد ،در شبکه های محلی سیمی وجود نداشته و باید دنبال راه کار ها و پروتکل های امنیتی باشیم که در صدد رفع و برآورده کردن نیاز های امنیتی خاص این شبکه ها باشد.

اتصال بی‌سیم، یک رسانه فیزیکی است و برای تأمین امنیت آن نمی‌توان تنها به وجود یک دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه‌های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آن‌ها، نوعی تهدید علیه شبکه به‌شمار می‌روند. علاوه بر این نقاط دسترسی، باید نگران لپ‌تاپ‌های بی‌سیم متصل به شبکه سیمی نیز باشیم. یافتن لپ‌تاپ‌های متصل به شبکه سیمی که یک کارت شبکه بی‌سیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب می‌شود. در اغلب موارد این لپ‌تاپ‌ها توسط SSID شبکه‌هایی را که قبلاً مورد دسترسی قرار داده‌اند، جست‌وجو می‌کنند و در صورت یافتن آن‌ها صرف‌نظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بی‌سیم در همسایگی شبکه فعلی قرار داشته باشد، به‌طور خودکار به آن وصل می‌شوند. به محض این‌که لپ‌تاپ به یک شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله‌ها به کار گیرند. در این شرایط علاوه

www.takbook.com

www.takbook.com

بر افشای اطلاعات مهم لپ‌تاپ، مهاجم می‌تواند از آن به عنوان نقطه شروعی برای حمله بـه شـبکه سـیمی استفاده کند. مهاجم درصورت انجام چنین اقداماتی، به‌طور کامل از دیواره آتش شبکه عبور می‌کند.

چنین نقطه ضعفی شبکه را به یک اسباب سرگرمی برای مهاجم تبدیل می‌کند. در حقیقت، نفوذ به چنین شبکه‌ای حتی نیازمند یک اسکن فعال یا حمله واقعی نیست. به واسطه ردیابی جریان اطلاعاتی یـک شـبکه بی‌سیم علاوه بر شناسایی توپولوژی بخش سیمی آن می‌توان اطلاعات مربوط به تجهیزات حیـاتی شـبکه و حتی گاهی اطلاعات مربوط به حساب‌های کاربری را به‌دست آورد.

با توجه به مطلاب گفته شده در بالا نیاز به پروتکل ها و تدابیر امنیتی ویژه ای داریم که خاص این شبکه ها باشد وبتوان امنیت در این شبکه ها را تامین کرد .در این ادامه تکنیک ها و روش های امن سازی این شبکه ها و پروتکل ها و استاندارد های امنیتی موجود را بررسی می کنیم.

www.takbook.com

www.takbook.com

فصل اول : معرفی شبکه های وای فای

Chapter One: Introduction Wi-Fi Networks

مراجع:[2],[1]

www.takbook.com

www.takbook.com

۱-۱ شبکه های Wi-Fiچیست؟

وای-فای(Wi-Fi)، مخفف عبارت Wireless Fidelity است و استانداردی از زیرمجموعه Bluetooth است و تحت آن ارتباطی با قدرتی بیشتر از خود Bluetooth ایجاد خواهد شد. ارتباط Wi-Fi بیشتر بر پایه ارتباط شبکه اینترنت به صورت بی سیم تاکید می کند و همین امر باعث محبوبیت بسیار زیاد آن شده است با استفاده از این تکنولوژی به راحتی در مسافرت، هواپیما و یا هتل می توان از طریق Laptop به اینترنت متصل شد. Wi-Fi ، که همان استاندارد IEEE802.11 است در مدل های 802.11a و802.11b مورد استفاده قرار می گیرد و استاندارد اصلی آن IEEE 802.11b است. در این مدل حداکثر سرعت انتقال اطلاعات ۱۱مگابیت برثانیه است و از فرکانس رادیویی ۲/٤ گیگاهرتز استفاده می کند. برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام 802.11b+ ایجاد شده که سرعت انتقال را تا ۲۲مگابیت بر ثانیه افزایش می دهد. در مدل 802.11a سرعت اطلاعات حدود ٥٤ مگابیت بر ثانیه است و از فرکانس ٥٠ گیگاهرتز استفاده می شود. به طور حتم این مدل در آینده ای نه چندان دور جای 802.11b را خواهد گرفت.

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 ٥٠ 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

www.takbook.com

www.takbook.com

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 802.11b و 802.11g کار می کنند و عمل ارسال و دریافت را بر روی فرکانس های ۲.٤ گیگاهرتزی و یا ۵ گیگا هرتزی انجام می دهند. اما واکی – تاکی های مذکور بر روی فرکانس ٤۹ 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 802.11a و 802.11g شامل تکنیک OFDM و برای استاندارد 802.11b ،شامل CCK می باشد.

۳) رادیو هایی که در سیستم Wi-Fi مورد استفاده قرار می گیرند، قابلیت تغییر فرکانس را دارا هستند. مزیت این ویژگی در آن است که موجب جلوگیری از ایجاد تداخل کار سیستم های مختلف Wi-Fi در نزدیکی هم می شود.

۱-۲ کاربردهای Wi-Fi

تکنولوژی Wi-Fi علاوه بر استفاده در ارتباط رایانه های شخصی در اتصال به اینترنت، به صورت بی سیم امکان استفاده از هر شبکه دیگری را نیز دارد. به عنوان نمونه در تلفن های همراه نسل جدید امکان اتصال به اینترنت از طریق Wi-Fi فراهم شده است. همچنین به عنوان راه حلی مؤثر به منظور توسعه شبکه های داخلی، بدون صرف هزینه سیم کشی مطرح شده است . دو تکنولوژی Wi-Fi و Bluetooth به عنوان رقبای یکدیگر در شبکه های بی سیم مطرح شده اند و هم اکنون نیز رقابت آنها در حال افزایش است،اما هدف این دو فناوری یکسان نبوده و هر کدام هدف جداگانه ای را در پیش گرفته اند.

بلوتوث برای استفاده در شبکه های بی سیم کوچک در نظر گرفته شده است که دارای مصرف پائین برق و برد کوتاه تری است اما Wi-Fi برای استفاده در شبکه های بی سیم متوسط با برد و پهنای باند وسیع تری مطرح شده است. تکنولوژی Wi-Fi در باندهای رادیویی ۲.٤ و ۵ گیگاهرتز فعال است و می تواند

www.takbook.com

www.takbook.com

سرعتی در حدود ۱۱Mbps تا ٥٤Mbps داشته باشد ، اما در مقابل Bluetooth تنها سرعتی در حدود ۷۲۰kbps را دارد. علاوه بر مواردی که در بالابه آن اشاره شد سرویس VOIP ،انتقال صدا از طریق تکنولوژی اینترنت ، که امکان برقراری تماس تلفنی روی شبکه های رایانه ای را مقدور می سازد نیز از Wi-Fi بهره می گیرد. با استفاده از Dual Mode Telephony دستگاه های تلفن همراه نیز قادر خواهند بود با استفاده از تکنولوژی Wi-Fi تماس هایی با کیفیت تکنولوژی سلولی را برقرار سازند و بدین ترتیب شما هم امکان اتصال به اینترنت را روی گوشی خود و هم امکان مکالمه تلفنی را خواهید داشت.

۱-۳ دلایل رشد Wi-Fi

شبکه های مبتنی بر Wi-Fi راه موفقیت و پیشرفت را در پیش گرفته است. تعداد کاربران تکنولوژی Wi-Fiکه در سال ۲۰۰۰ در حدود ۲/۵ میلیون نفر بود اکنون به ۱۸ میلیون کاربر رسیده است و می رود تا مسیر رشد و پیشرفت خود را ادامه دهد، از مهم ترین دلایل رشد تکنولوژی Wi-Fi می توان به موارد زیر اشاره کرد:

۱ـ پشتیبانی شرکت های مختلف: شرکت های بزرگ و معتبری همچون مایکرو سافت، اینتل، سیسکو و آی بی ام بشدت مشغول کار روی تکنولوژی Wi-Fi هستند و سرمایه گذاری های هنگفتی نیز در این زمینه انجام داده اند به عنوان نمونه شرکت اینتل سیصدمیلیون دلار برای توسعه صنعت Wi-Fi بر روی Centrino سرمایه گذاری کرده است.

۲ـ توسعه ارتباطات باند پهن: استفاده از فناوری Wi-Fi سبب توسعه شبکه های باندپهن شده است به گونه ای که در سال جاری حدود ۳۰ درصد رشد در زمینه باندپهن مشاهده شده است.

۳ـ شبکه های بزرگ ملی: هم اکنون در برخی از کشورهای دنیا شبکه های بزرگ و ملی Wi-Fi در حال فعالیت هستند به عنوان نمونه در کشور آمریکا چهار شبکه cometa Networks،voice stream، Toshiba و Boingo مشغول سرویس دهی به کاربران هستند.

٤ـ تجهیزات آماده: شرکت های تولیدکننده سخت افزار در سال های اخیر همراه با سخت افزارهای خود لوازم و متعلقات مورد نیاز سیستم های Wi-Fi را نیز به صورت آماده در اختیار مشتریان قرار می دهند و دیگر نیازی به تهیه این وسایل از بازارهای رایانه به صورت جداگانه وجود ندارد. هم اکنون شرکت های TIVO، Toshiba، Dell و ... در رایانه ها و قطعات تولیدی خود تکنولوژی Wi-Fi را گنجانده اند.

www.takbook.com

www.takbook.com

۵ـ گسترش شبکه: پیشگامان صنعت Wi-Fi در همه نقاط دنیا بشدت در حال توسعه شبکه ها هستند، به عنوان نمونه در پارک ها، رستوران ها، اماکن تفریحی و گردشگری این تکنولوژی به چشم می خورد.

٦ ـ کاهش قیمت ها: هم اکنون قیمت تجهیزات Wi-Fi در نقاط مختلف دنیا سیر نزولی را آغاز کرده است و به نصف کاهش یافته است و همین کاهش قیمت ها سبب گرایش بیشتر افراد به سوی تکنولوژی Wi-Fi خواهد شد.

۷ـ نوآوری های بیشتر: تکنولوژی Wi-Fi به دلیل تازه وارد بودن به سرعت در حال پیشرفت است. شرکت های اینتل و Mash Networks در حال ساخت آنتن هایی هستند که نسبت به آنتن های فعلی محدوده بیشتری را پوشش می دهد به علاوه شرکت های سازنده گوشی تلفن همراه نیز در حال ساخت گوشی هایی با امکانات Wi-Fi می باشند.

۸– هزینه: تجهیزات مورد استفاده در شبکه های کابلی نسبت به تجهیزات مورد استفاده در شبکه های بی سیم ارزان تر است اما با توجه به رشد روزافزون شبکه های بی سیم قیمت تجهیزات آن نیز در حال کاهش است.

۹– کارآیی: شبکه های کابلی دارای بالاترین کارآیی هستند، ابتدا پهنای باند ۱۰Mbps در این شبکه ها رواج داشت اما با گذشت زمان این سرعت به پهنای باند ۱۰۰Mbps و سپس ۱۰۰۰ Mbps افزایش یافت. هم اکنون سوئیچ هایی با پهنای باند ۱Gbps در بازار وجود دارد. اما در مقابل شبکه های بی سیم با استاندارد 802.11b وحداکثر ۱۱Mbps و با استاندارد a۸۰۲.۱۱ پهنای باندی در حدود ٥٤Mbps دارد و در استانداردهای جدید این سرعت به ۱۰۸Mbps افزایش یافته است. علاوه بر فاکتور سرعت و پهنای باند، فاصله نیز از ملاک های مهم در سرعت ارسال داده ها در شبکه ها می باشد. با توجه به این که فناوری Wi-Fi به فاصله حساس می باشد و تنها در فواصل زیر یکصدمتر قابل به سرویس دهی می باشد، نباید از این تکنولوژی در فواصل بالای یکصدمتر و یا در مکان هایی که موانع فیزیکی دارد استفاده کرد.

۱۰– اطمینان پذیری: شبکه های کابلی در مقابل شبکه های بی سیم از اطمینان بیشتری برخوردار هستند اما در موقع راه اندازی باید تجهیزات را به درستی نصب کرد تا در آینده مشکلی در سرویس دهی شبکه به وجود نیاید، به علاوه تجهیزات بی سیم مشکلات خاص خود مانند قطع شدن های پیاپی، تداخل امواج الکترومغناطیسی ـ تداخل با شبکه های بی سیم مجاور و غیره را دارند که روند رو به رشد آن بیانگر بهبود ضعف ها و کمبودها در شبکه است.

www.takbook.com

www.takbook.com

۱۱- امنیت: در شبکه های کابلی به دلیل firewall امنیت بیشتری وجود دارد در حالی که در شبکه های بی سیم به دلیل استفاده از هوا به عنوان بستری برای انتقال اطلاعات، بدون داشتن تکنیک خاصی برای رمزنگاری و نیز رمزگشایی اطلاعات، امنیت اطلاعات به خطر می افتد و لزوم به کارگیری تکنیک های رمزنگاری WEP (wired Equivalent privacy) سبب افزایش امنیت اطلاعات در این شبکه ها می شود.

۱-٤ ترکیب سیستم Wi-Fi با رایانه

امروزه اغلب رایانه های لپ تاپ مجهز به سیستم Wi-Fi داخلی هستند و در غیر این صورت نیازمند نصب یک کارت Wi-Fi بر روی لپ تاپ و یا رایانه رومیزی خود خواهیم بود. شما می توانید یک کارت Wi-Fi در سیستم 802.11aیا 802.11b و یا 802.11g تهیه کنید که البته نوع 802.11g نسبت به تجهزات 802.11b از سرعت بالاتری برخوردار است. برای لپ تاپ ها این تجهیزات در قالب کارت های PCMCIA که در محل مخصوص خود نصب می شوند و یا به صورت اتصال خارجی از طریق یک درگاه USB عرضه می شوند.

برای رایانه های رومیزی، می توانید از کارت های PCI و یا درگاه USB برای این منظور استفاده کنید. پس از نصب این تجهیزات کاربر قادر است تا در مکان هایی که اینترنت به شکل بدون سیم ارائه می شود با داشتن یک اشتراک، از خدمات بهره گرفته و به شبکه متصل شود.

۱-۵ شبکه Wi-Fi چگونه کار می کنند؟

دو نوع مد عملیات برای برقرای ارتباطات ،در این استاندارد وجود دارد ،حالت دارای زیر ساخت [۱] و حالت بدون زیر ساخت یا موردی[۲].در حالت دارای زیر ساخت یک کدام از نود های شرکت کننده در شبکه به عنوان نقطه دسترسی عمل می کند و سایر نود ها برای ارتباط با یک دیگر ،ابتدا باید با نقطه دسترسی ارتباط برقرار کنند ،در حالت بدون زیر ساخت هیچ گونه نود مرکزی و نقطه دسترسی وجود ندارد و نود ها برای ارتباط با یک دیگر به طور مستقیم عمل می کنند و احتمالا از نود های دیگر نیز می توانند برای کمک در مسیر یابی استفاده کنند .نمونه ای از این شبکه ها در تصاویر ۱.۱ و ۱.۲ نشان داده شده است.

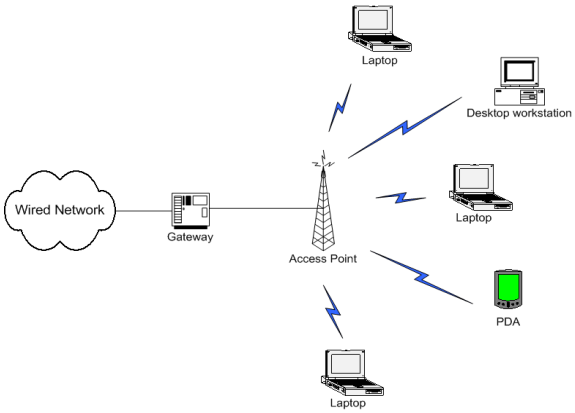
---

[۱] *Infrastructure-based*

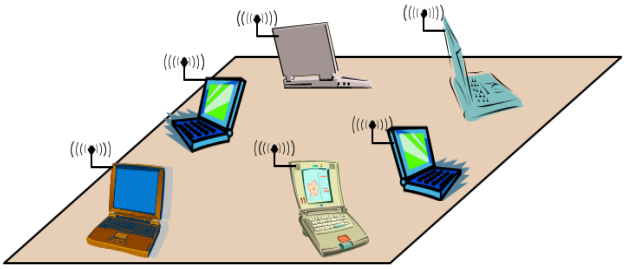
[۲] *Ad hoc*

www.takbook.com

www.takbook.com



شکل ۱.۱:ساختار شبکه های بی سیم در حالت دارای زیر ساخت



شکل ۱.۲:ساختار شبکه های بی سیم در حالت بدون زیر ساخت

برای پشتیبانی ارتباطات بی سیم کلاینت ها و نقطه دسترسی شامل یک رادیو و آنتن می باشند،ایده اصلی مورد استفاده در استاندارد IEEE802.11 برای شناسایی و ارتباطات ایستگاه ها با یک دیگر استفاده از فریم هایی به نام Beacon و Request/ Release می باشد،فریم های Beacon در هر ثانیه ده بار توسط نقطه دسترسی به تمام ایستگاه ها ارسال می شود و به این ترتیب نقطه دسترسی خود را به ایستگاه ها معرفی می کند و آنها قادر خواهند بود به راحتی نقطه دسترسی را شناسایی کنند ،همچنین ایستگاه ههها یا کلاینت ها با ارسال فریم هایی Broadcast به نام probe Broadcast خود را به نقطه دسترسی معرفی می کنند و نقطه دسترسی نیز در پاسخ به آن ایستگاه یک فریم پاسخ به ایستگاه ارسال می کند که به عنوان تصدیقی برای شناسایی آن ایستگاه از جانب نقطه دسترسی محسوب می شود.

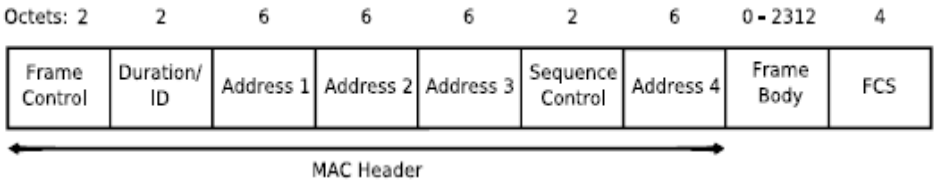
۱-۶ تحلیل ترافیک شبکه های Wi-Fi

هر بسته انتقالی در شبکه هایWi-fi شامل بیت های می شود که در لایه های مختلف برای ارتباطات استفاده می شود ،هر چند که ممکن است است بسته ها در این نوع شبکه ها رمز نگاری شوند ،ولی همیشه دارای هدر های هستند که رمز نمی شوند ،در نتیجه هدر بسته ها برای همه قابل دسترس خواهد بود و

www.takbook.com

www.takbook.com

مهاجمین قادرند که ترافیک شبکه را آنالیز کنند .تمام بسته ها در شبکه های Wi-Fi با ساختار بسته های MAC مطابقت می کنند، ساختار قاب های MAC در شکل ۱.۳ نمایش داده شده است.



شکل ۳.۱: ساختار قاب MAC

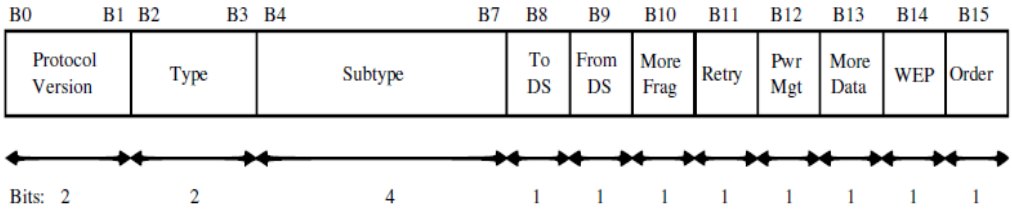
فیلد Frame Control برای مشخص کردن نوع داده بسته به کار می رود،به طور کلی سه نوع داده و تعداد بسیار زیادی زیر نوع وجود دارد که در زیر لیت شده است:

۱.مدیریتی:.Association, Probe, Beacon, Authentication

۲.کنترلی:.RTS, CTS, PS-Poll, ACK, CF-Ack/Poll

۳.داده:.Data, Data + CF-Ack/Poll and Null-function

در شکل زیر ساختار بیتی فیلد Frame Control نمایش داده شده است :



شکل ٤.۱: ساختار فیلد frame control

اگر شبکه قسمتی از شبکه های بی سیم توزیع شده باشد (WDS[۳]) آنگاه :

FromDS = 1 و ToDS = 1

اگر شبکه در مد موردی یا بدون زیر ساخت باشد انگاه :

ToDS = 0 , FromDS = 0, Type = Data

اگر شبکه در مد دارای زیر ساخت باشد آنگاه :

ToDS =1 , FromDS = 0, Type = Data

به طور کلی پنج نوع آدرس در این بسته ها ممکن است به کار روند که عبارتند از :

[۳] *Wireless Distributed System*

www.takbook.com

www.takbook.com

آدرس مقصد(DA): گیرنده نهایی بسته را مشخص می کند.

آدرس مبدا(SA):گیرنده ابتدایی بسته را مشخص می کند

آدرس دریافت کننده(RA):ادرس نقطه دسترسی گیرنده بعدی بسته را مشخص می کند.

آدرس انتقال دهنده(TA):آدرس نقطه دسترسی قبلی که بسته را فرستاده است، مشخص می کند.

شناسه BSS[٤]:نقطه دسترسی را در یک BSS مشخص می کند

نحوه قرار گیری این آدرس ها بسته مقادیر فیلد های ToDSوFromDS می باشد که در شکل زیر نمایش داده شده است.

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	n/a
0	1	DA	BSSID	SA	n/a
1	0	BSSID	SA	DA	n/a
1	1	RA	TA	DA	SA

شکل ۵.۱:فیلد های ادرس در فریم MAC

هر فریم دریافتی شامل قدرت سیگنال دریافتی می باشد که توسط رادیوی گیرنده محاسبه می شود که از ترکیب این اطلاعات با اطلاعات GPS می توان برای به دست آوردن محدوه شبکه، محل قرارگیری نقطه دسترسی و به دست آوردن محل کلاینت مورد استفاده قرار گیرد. اطلاعات تحلیلی به دست آمده از فریم های دریافت شده در شکل زیر دسته بندی شده است:

Fact	Frame	Requirements
WDS	Data	1 frame
Ad-hoc/Infrastructure	Beacon/Probe/Data	1 frame
Network range	Any	3 frames and GPS
Client/Access point location	Any	3 frames and GPS
WEP	Beacon/Probe/Data	1 frame
WPA	Beacon/Probe/Data	1 frame
SSID	Beacon/Probe	1 frame
Access point MAC address	Any	1 frame
Client MAC address	Probe Request/Data	1 frame
Wired client MAC address	Data	1 frame
Contents of data	Data	Intelligent guess

شکل ٦.۱:اطلاعات قابل دسترس از تحلیل بسته های WI-Fi

[٤] *Basic Service set*

www.takbook.com

www.takbook.com

۱-۷ آینده شبکه های Wi-Fi

WiMAX استاندارد دیگری است که توسط IEEE 802.16مطرح شده و ارتباطات بی سیم تا شعاعی در حدود ۵۰ کیلومتر و پهنای باندی حدود ۷۰Mbps را فراهم میکند. این یک تکنولوژی جدید، بسیار مؤثر و کارا بوده و قدم بزرگتری بر فراز WiFi است.

آنچه بنظر می رسد آنست که بزودی شاهد موبایل هایی مجهز به تکنولوژی WiFi در فروشگاه ها خواهیم بود. این تکنولوژی فرصتهای کاری جدید بسیاری را برای اپراتورهای موبایل و سازنده های گوشی موبایل ایجاد خواهد کرد.

سرویس هایی نظیر Push Email،VoIP و IMS و ... همه نسبت به آنچه احتمالاً اکنون ارائه می شوند ارزانتر خواهند شد و میزان بازده و کارایی این تکنولوژی می تواند ترافیک شبکه های موبایل را کاهش دهد.

۱-۸ نتیجه گیری

با توجه به تمامی ویژگی های مثبت شبکه های Wi-Fi و امکاناتی خوبی که به ارمغان می آورد باید توجه داشت که 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 باید مطمئن بود. 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.

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 ،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 حتی برنامه های نظامی و نمایشگاه ها و دفاتر استیجاری نیز در فهرست موارد کاربرد شبکه های بی سیم قرار دارند.

www.takbook.com

www.takbook.com

۲ فصل دوم : استاندارد های شبکه محلی بی سیم

Chapter Two: The 802.11 Standard Defined

مراجع:**[3],[4],[5],[6],[7],[8]**

www.takbook.com

www.takbook.com

۲-۱ معرفی

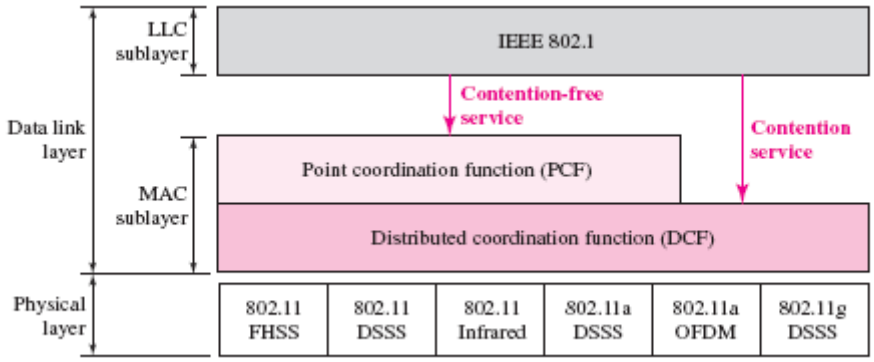
امروزه با بهبود عملکرد، کارایی و عوامل امنیتی، شبکه های بیسیم به شکل قابل توجهی در حال رشد و گسترش هستند و استاندارد IEEE 802.11 استاندارد بنیادی است که شبکه های بیسیم بر مبنای آن طراحی و پیاده سازی می شوند. در ماه ژوئن سال ۱۹۹۷ انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11-1997 را به عنوان اولین استاندارد شبکه های محلی بیسیم منتشر ساخت. این استاندارد در سال ۱۹۹۹ مجددا بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE 802.11-1999 منتشر شد. استاندارد جاری شبکه های محلی بیسیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999، توسط سازمان استاندارد سازی بین المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال ۱۹۹۷، شکل گیری و پیدایش شبکه سازی محلی بیسیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد ۱۹۹۷، پهنای باند ۲Mbps را تعریف می کند با این ویژگی که در شرایط نامساعد و محیط های دارای اغتشاش (نویز) این پهنای باند می تواند به مقدار ۱Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند ۱Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط های عاری از اغتشاش (نویز) پهنای باند ۲Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی GHz ۲.٤ عمل می کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون های رادیویی DSSS و FHSS به عنوان رسانه انتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتا محدود و نادر است. گروه کاری ۸۰۲.۱۱ به زیر گروه های متعددی تقسیم می شود. برخی از مهم ترین زیر گروه ها به قرار زیر است:

-802.11D: Additional Regulatory Domains
-802.11E: Quality of Service (QoS)
-802.11F: Inter-Access Point Protocol (IAPP)
-802.11G: Higher Data Rates at 2.4 GHz
-802.11H: Dynamic Channel Selection and Transmission Power Control
- 802.11i: Authentication and Security

شکل زیر گروه های کاری در لایه فیزیکی در استاندارد ۸۰۲.۱۱ را نمایش می دهد.

www.takbook.com

www.takbook.com



شکل ۲.۱:جایگاه استاندارد ۸۰۲.۱۱

کمیته e ۸۰۲.۱۱ کمیته ای است که سعی دارد قابلیت QoS اتـرنت را در محیط شبکه های بیسـیم ارائـه کند. توجه داشته باشید که فعالیت های این گروه تمام گونه های ۸۰۲.۱۱ شامل a، b، و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی سیم بیاورد.

کمیته g ۸۰۲.۱۱ کمیته ای است که با عنوان ۸۰۲.۱۱ توسعه یافته نیز شناخته می شود. این کمیته در نظـر دارد نرخ ارسال داده ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صـنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲٤۰۰ مگاهرتز تا ۲٤۸۳.۵ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشـع رادیـویی نیـازی بـه مجوز ندارد. استاندارد g ۸۰۲.۱۱ تا کنون نهایی نشده است و مهم ترین علت آن رقابت شدید میان تکنیـک های مدولاسیون است. اعضاء این کمیته و سازندگان تراشه توافق کرده انـد کـه از تکنیـک تسـهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می تواند به عنوان یک روش جـایگزین و رقیـب مطـرح باشد.

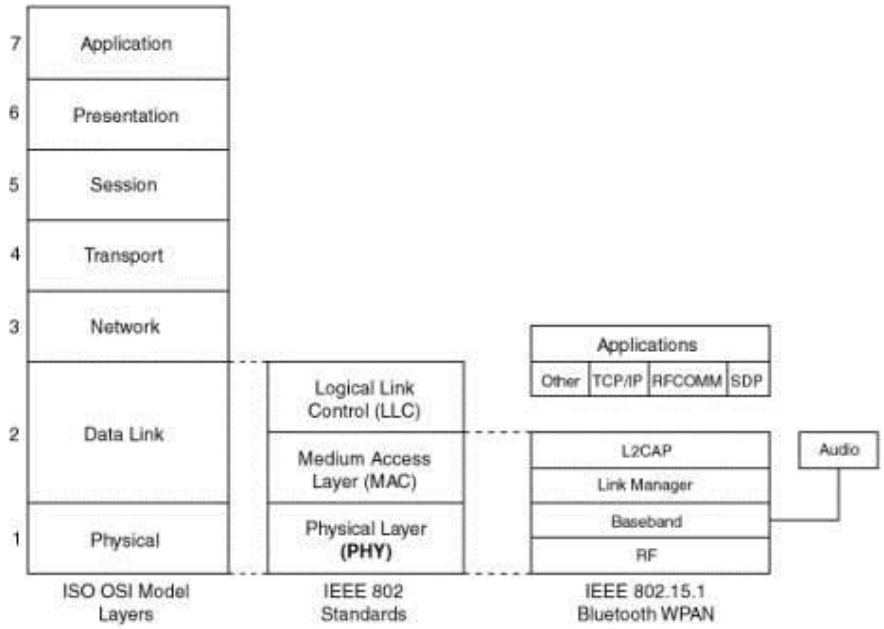
کمیته h ۸۰۲.۱۱ مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصـرفی و نیـز تـوان امـواج ارسالی توسط فرستنده های مبتنی بر ۸۰۲.۱۱ است.

فعالیت دو کمیته i ۸۰۲.۱۱و x ۸۰۲.۱۱ در ابتدا برروی سیستم های مبتنی بـر b ۸۰۲.۱۱ تمرکـز داشـت. این دو کمیته مسئول تهیه پروتکل های جدید امنیت هستند. استاندارد اولیه از الگوریتمی موسـوم بـه WEP استفاده می کند که در آن دو ساختار کلید رمز نگاری به طول ٤۰ و ۱۲۸ بیـت وجـود دارد. WEP مشخصـا یک روش رمزنگاری است که از الگوریتم RC4 برای رمزنگاری فریم ها استفاده می کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه های محلی بیسیم است.

این استاندارد لایه های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی بـا اتصال بیسیم را در بر دارد. شکل ۲.۲ جایگاه استاندارد ۸۰۲.۱۱ را در مقایسه با مدل مرجع نشان می دهد.

www.takbook.com

www.takbook.com



شکل ۲.۲:مقایسه استاندارد ۸۰۲.۱۱ با استاندارد مرجع OSI

محیط های بیسیم دارای خصوصیات و ویژگی های منحصر به فردی می باشند که در مقایسه با شبکه های محلی سیمی جایگاه خاصی را به این گونه شبکه ها می بخشد. به طور مشخص ویژگی های فیزیکی یک شبکه محلی بیسیم محدودیت های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت ها، استاندارد شبکه های محلی بیسیم را وا می دارد که فرضیات خود را بر پایه یک ارتباط محلی و با برد کوتاه بنا نهد. پوشش های جغرافیایی وسیعتر از طریق اتصال شبکه های محلی بیسیم کوچک برپا می شود که در حکم عناصر ساختمانی شبکه گسترده هستند. سیار بودن ایستگاه های کاری بیسیم نیز از دیگر ویژگی های مهم شبکه های محلی بیسیم است. در حقیقت اگر در یک شبکه محلی بیسیم ایستگاه های کاری قادر نباشند در یک محدوده عملیاتی قابل قبول و همچنین میان سایر شبکه های بیسیم تحرک داشته باشد، استفاده از شبکه های محلی بیسیم توجیه کاربردی مناسبی نخواهد داشت.

از سوی دیگر به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایه دسترسی به رسانه (MAC) در استاندارد ۸۰۲.۱۱ می بایست از دید لایه های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیار بودن ایستگاه های کاری را به گونهای شفاف پوشش دهد که از دید لایه های بالاتر استاندارد این سیاربودن احساس نشود. این نکته سبب می شود که لایهMAC در این استاندارد وظایفی را بر عهده بگیرد که معمولا توسط لایه های بالاتر شبکه انجام می شوند. در واقع این استاندارد لایه های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می کند و به طور مشخص لایه فیزیکی جدید از فرکانس های رادیویی به عنوان رسانه انتقال بهره می برد.

www.takbook.com

www.takbook.com

۲-۲ معماری شبکه های محلی بی سیم

معماری ۸۰۲.۱۱ از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سیار بودن ایستگاه های کاری را پنهان از دید لایه های فوقانی برآورده می سازد. ایستگاه بیسیم یا به اختصار ایستگاه (STA)، بنیادی ترین عنصر ساختمانی در یک شبکه محلی بیسیم است. یک ایستگاه، دستگاهی است که بر اساس تعاریف و پروتکل های ۸۰۲.۱۱ (لایه های MAC و PHY) عمل کرده و به رسانه بیسیم متصل است. توجه داشته باشید که براساس تعریف کلاسیک شبکه های کامپیوتری، یک شبکه کامپیوتری مجموعه ای از کامپیوترهای مستقل و متصل است که منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام ها است. ایستگاه های کاری بیسیم امروزی عمدتا به صورت مجموعه سخت افزاری/نرم افزاری کارت های شبکه بیسیم پیاده سازی می شوند. همچنین یک ایستگاه می تواند یک کامپیوتر قابل حمل، کامپیوتر جیبی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقع در حکم پلی است که ارتباط ایستگاه های بیسیم را با سیستم توزیع یا شبکه سیمی برقرار می سازد. کوچکترین عنصر ساختمانی شبکه های محلی بیسیم در استاندارد ۸۰۲.۱۱ مجموعه سرویس پایه یا BSS نامیده می شود. در واقع BSS مجموعه ای از ایستگاه های بیسیم است.

۲-۲-۱ همبندی های ۸۰۲.۱۱

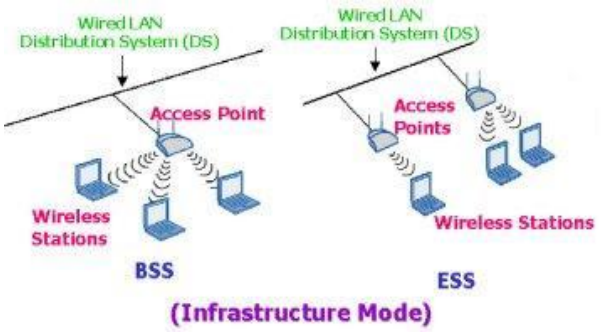
در یک تقسیم بندی کلی می توان دو همبندی را برای شبکه های محلی بیسیم در نظر گرفت. ساده ترین همبندی، فی البداهه (Ad Hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲.۱۱، IBSS است. در این همبندی ایستگاه ها از طریق رسانه بیسیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیزات یا ایستگاه واسطی استفاده نمی کنند. واضح است که در این همبندی به سبب محدودیت های فاصله هر ایستگاهی ضرورتا نمی تواند با تمام ایستگاه های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبندی IBSS آن است که ایستگاه ها در محدوده عملیاتی بیسیم یا همان برد شبکه بیسیم قرار داشته باشند. شکل ۲.۳ همبندی IBSS را نشان می دهد.

شکل ۲.۳ :ساختار شبکه در حالت موردی

www.takbook.com

www.takbook.com

همبندی دیگر زیرساختار است. در این همبندی عنصر خاصی موسوم بـه نقطـه دسترسـی وجـود دارد. نقطه دسترسی ایستگاه های موجود در یک مجموعه سرویس را به سیستم توزیع متصل می کند. در این هم بندی تمام ایستگاه ها با نقطه دسترسی تماس می گیرند و اتصال مستقیم بین ایستگاه هـا وجـود نـدارد در واقع نقطه دسترسی وظیفه دارد فریم ها (قاب های داده) را بین ایستگاه ها توزیع و پخش کند. شـکل ۲-۲ همبندی زیرساختار را نشان می دهد.



شکل ۲.٤ : همبندی زیرساختار در دوگونه BSS و ESS

در این هم بندی سیستم توزیع، رسانه ای است که از طریـق آن نقطـه دسترسـی (AP) بـا سـایر نقـاط دسترسی در تماس است و از طریق آن می تواند فریم ها را به سایر ایستگاه ها ارسال نماید. از سوی دیگـر می تواند بسته ها را در اختیار ایستگاه های متصل بـه شـبکه سـیمی نیـز قـرار دهـد. در اسـتاندارد ۸۰۲.۱۱ توصیف ویژه ای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجـود ندارد، در واقع این استاندارد تنها خدماتی را معین می کند که سیستم توزیع می بایست ارائه نماید. بنـابراین سیستم توزیع می تواند یک شبکه ۸۰۲.۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظـر را فراهم می کند.

استاندارد ۸۰۲.۱۱ با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش می دهد. این همبندی به شکل مجموعه سرویس گسترش یافته (ESS) بر پا مـی شـود. در ایـن روش یـک مجموعـه گسـترده و متشکل از چندین BSS یا مجموعه سرویس پایه از طریق نقاط دسترسی با یکدیگر در تماس هسـتند و بـه این ترتیب ترافیک داده بین مجموعه های سرویس پایه مبادله شده و انتقال پیام ها شکل می گیـرد. در ایـن همبندی ایستگاه ها می توانند در محدوده عملیاتی بزرگ تری گردش نمایند. ارتباط بین نقـاط دسترسـی از طریق سیستم توزیع فراهم می شود. در واقع سیستم توزیع ستون فقرات شبکه های محلی بیسیم است و می تواند با استفاده از فناوری بیسیم یا شبکه های سیمی شکل گیرد. سیستم توزیع در هـر نقطـه دسترسـی بـه عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می باشد. نکته

www.takbook.com

www.takbook.com

قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه های سیار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه MAC تلقی می کنند. به این ترتیب پروتکل های رایج شبکه های کامپیوتری کوچکترین تأثیری از سیار بودن ایستگاه ها و رسانه بیسیم نمی پذیرند. جدول ۲.۱ همبندی های رایج در شبکه های بیسیم مبتنی بر ۸۰۲.۱۱ را به اختصار جمع بندی می کند.

802.11 Topologies		
Independent Basic Service Set (IBSS) ("Ad Hoc" or "Peer to Peer")	Infrastructure	
	Basic Service Set (BSS)	Extended Service Set (ESS)

جدول ۲.۱: همبندی های رایج در استاندارد ۸۰۲.۱۱

۲-۳ خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه های کاری پیاده سازی می شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲.۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه های سیمی، در شبکه های بیسیم قابل اعمال نیست استاندارد ۸۰۲.۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می نماید. سرویس هویت سنجی به ایستگاه کاری امکان می دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بیسیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۸۰۲.۱۱ دو گونه خدمت هویت سنجی را تعریف می کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحلهای است. در ابتدا ایستگاهی که می خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می کند. ایستگاه گیرنده نیز فریمی در پاسخ می فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده تر است و فرض می کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهره گیری از

www.takbook.com

www.takbook.com

پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقا مجاز به استفاده از شبکه بوده است، قطع می گردد.

در یک شبکه بی سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک دادهای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بیسیم را تحت تأثیر قرار می دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه های سیمی نماید.

۲-٤ خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی های مبتنی بر سیستم توزیع را مهیا می سازد. معمولا خدمات توزیع توسط نقطه دسترسی فراهم می شوند. خدمات توزیع در این استاندارد عبارتند از:

- پیوستن به شبکه
- خروج از شبکه بی سیم
- پیوستن مجدد
- توزیع
- مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیار و نقطه دسترسی فراهم می کند. هر ایستگاه کاری قبل از ارسال داده می بایست با یک نقطه دسترسی برروی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می دهد که فریم های ارسال شده به سمت ایستگاه سیار را به درستی در اختیارش قرار دهد. خروج از شبکه بیسیم هنگامی بکار می رود که بخواهیم اجبارا ارتباط ایستگاه سیار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی سیم" است با این تفاوت که در این سرویس ایستگاه سیار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می کند که با نقطه دسترسی قبلی تماس گرفته و فریم

www.takbook.com

www.takbook.com

های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیار فرستاده شده اند. با استفاده از سرویس توزیع فریم های لایه MAC به مقصد مورد نظرشان می رسند. مجتمع سازی سرویسی است که شبکه محلی بیسیم را به سایر شبکه های محلی و یا یک یا چند شبکه محلی بیسیم دیگر متصل می کند. سرویس مجتمع سازی فریم های ۸۰۲.۱۱ را به فریم هایی ترجمه می کند که بتوانند در سایر شبکه ها (به عنوان مثال ۸۰۲.۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم های سایر شبکه ها نیز به فریم های ۸۰۲.۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه های کاری سیار قرار می گیرند.

۲-۵ دسترسی به رسانه

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی به روش دسترسی CSMA/CD شباهت دارد. در این روش ایستگاه های کاری قبل از ارسال داده کانال رادیویی را کنترل می کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه یک زمان تصادفی صبر کرده و مجددا اقدام به کنترل کانال رادیویی می کنند. در روش CSMA/CA ایستگاه فرستنده ابتدا کانال فرکانسی را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد اقدام به ارسال می کند. گیرنده فیلد کنترلی فریم یا همان CRC را چک می کند و سپس یک فریم تصدیق می فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجددا فریم را ارسال می کند. این عمل تا زمانی ادامه می یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم ها به تعداد آستان های مشخصی برسد که پس از آن فرستنده فریم را دور می اندازد.

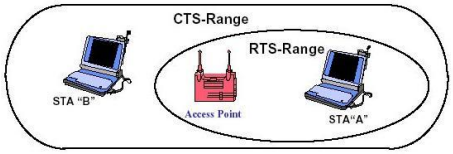
در شبکه های بیسیم بر خلاف اترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می شود.

در یک شبکه بی سیم، بر خلاف شبکه های سیمی، نمی توان فرض کرد که تمام ایستگاه های سیار امواج یکدیگر را دریافت می کنند. در واقع در محیط بیسیم حالاتی قابل تصور است که به آنها نقاط پنهان می گوییم. در شکل زیر ایستگاه های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.

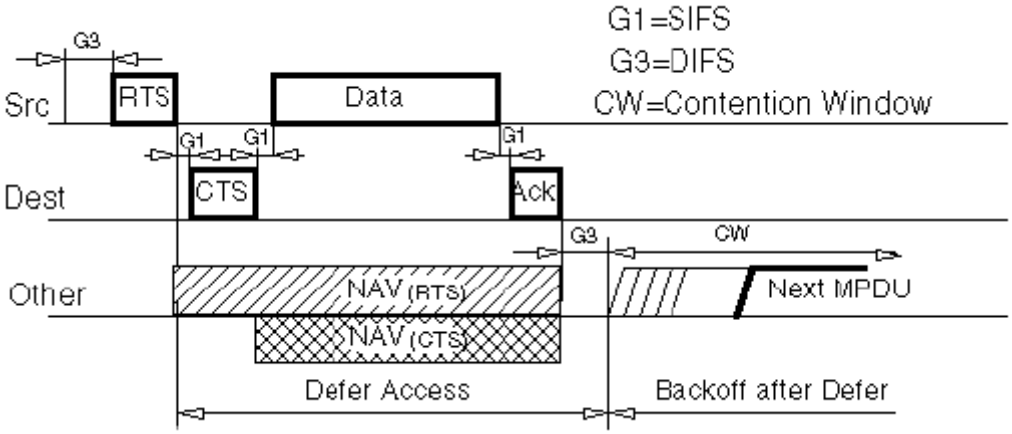
www.takbook.com

www.takbook.com



شکل ۲.۵ :روزنه ها پنهان

برای غلبه بر این مشکل، استاندارد ۸۰۲.۱۱ از تکنیکی موسوم به اجتناب از تصادم و مکانیزم تصدیق استفاده می کند. همچنین با توجه به احتمال بروز روزنه های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به شنود مجازی رسانه یا VCS استفاده می شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می فرستد. هنگامی که گیرنده این فریم را دریافت می کند، رسانه را کنترل می کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می کند. تمام ایستگاه هایی که فریم های کنترلی RTS/CTS را دریافت می کنند وضعیت کنترل رسانه خود موسوم به شاخص NAV را تنظیم می کنند. در صورتی که سایر ایستگاه ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می کنند که مرتبا به صورت پویا تغییر می کند. به این ترتیب مشکل روزنه های پنهان حل شده و تصادم ها نیز به حداقل مقدار می رسند. شکل ۲-٤ زمان بندی RTS/CTS و وضعیت سایر ایستگاه ها را نشان می دهد.



شکل ۲.٦ : زمان بندی RTS/CTS

www.takbook.com

www.takbook.com

۲-۵-۱ لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می دهد. اول آنکه رابطی برای تبادل فریم های لایه MAC جهت ارسال و دریافت داده ها فراهم می کند. دوم اینکه با استفاده از روش های تسهیم فریم های داده را ارسال می کند و در نهایت وضعیت رسانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار می دهد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر می باشند:

۱.استفاده از تکنیک رادیویی DSSS

۲.استفاده از تکنیک رادیویی FHSS

۳.استفاده از امواج رادیویی مادون قرمز

در این استاندار لایه فیزیکی می تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون ۱٦-PPM و ٤-PPM مبادله می شوند.

۲-۵-۱-۱ ویژگی های سیگنال های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی های جالب توجه سیگنال های طیف گسترده نهفته است. این ویژگی های عبارتند از:

۱.مصونیت بالا در مقابل پارازیت و تداخل

۲.رسایی با تفکیک پذیری و دقت بالا

۳.امکان استفاده در CDMA

٤. پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می رسد.

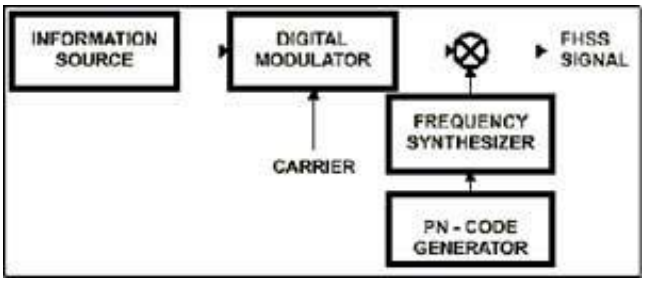
مزایای فوق کمیسیون FCC را بر آن داشت که در سال ۱۹۸۵ مجوز استفاده از این سیگنال ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

www.takbook.com

www.takbook.com

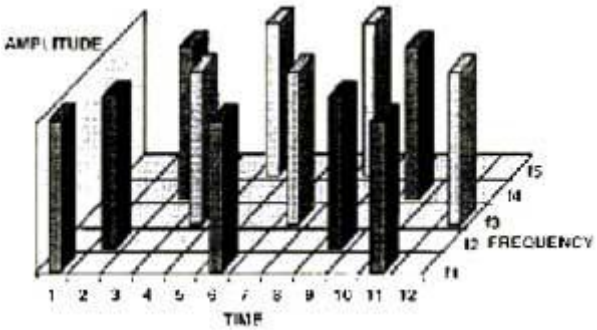
۲-۵-۱-۲ سیگنال های طیف گسترده با جهش فرکانسی

در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می کند. شکل ۲-۵ این تکنیک را در قالب یک نمودار نشان می دهد.



شکل ۲.۷: تکنیک FHSS =Pseudonoise code PN-CODE

در این شکل سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ تری در مقایسه با سیگنال اطلاعات انتخاب می شود. با توجه به اینکه فرکانس های pn-code با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملا تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می گوییم.



شکل ۲.۸ : تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

بر اساسی مقررات FCC و سازمان های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ٤٠٠ میلی ثانیه است که برابر با حداقل ۲.۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲.۱۱ حداقل فرکانس جهش در آمریکای شمالی و اروپا ٦ مگاهرتز و در ژاپن ۵ مگاهرتز می باشد.

www.takbook.com

www.takbook.com

۲-۵-۱-۳ سیگنال های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال برروی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کد به گونه ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کد تسهیم می شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می گردد. در استاندارد ۸۰۲.۱۱ روش مدولاسیون مورد استفاده در سیستم های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تسهیم می شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد ۸۰۲.۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می شود، داده های خام به صورت تفاضلی تسهیم شده و ارسال می شوند و در گیرنده نیز یک آشکار ساز تفاضلی سیگنال های داده را دریافت می کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال های داده تغییر می کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت های داده تغییر می کند. جدول زیر ایده مدولاسیون فاز را نشان می دهد.

Symbols	Bits	Phase Modulation
1	00	$A\sin(\omega t+\theta_1)$
2	01	$A\sin(\omega t+\theta_2)$
3	10	$A\sin(\omega t+\theta_3)$
4	11	$A\sin(\omega t+\theta_4)$

شکل ۲.۹ : مدلاسیون فاز

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می گیرند و چهار نماد را پدید می آورند. واضح است که در این روش تسهیم، دامنه سیگنال ثابت است. در روش تسهیم تفاضلی سیگنال اطلاعات با توجه به میزان اختلاف فاز و نه مقدار مطلق فاز تسهیم و مخابره می شوند. به عنوان مثال در روش pi/4-DQPSK، چهار مقدار تغییر فاز pi/4-۳، 3pi/4، pi/4، و pi/4- است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می تواند دو بیت را کدگذاری نماید.

www.takbook.com

www.takbook.com

اختلاف فاز	بیتهای زوج	بیتهای فرد
-3pi/4	1	1
3 pi/4	1	0
Pi/4	0	0
-pi/4	0	1

شکل ۲.۱۰ : مدولاسیون تفاضلی

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیما توسط یک دنباله از کدهای شبه تصادفی تسهیم می شود. در این تکنیک نرخ بیتی شبه کد تصادفی، نرخ تراشه نامیده می شود. در استاندارد ۸۰۲.۱۱ از کدی موسوم به کد بارکر برای تولید کدها تراشه سیستم DSSS استفاده می شود. مهم ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

جدول زیر فهرست کامل کدهای بارکر را نشان می دهد. همانگونه که در این جدول مشاهده می شود کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار می گیرد، از کد بارکر با طول ۱۱ (N=11) استفاده می شود. این کد به ازاء یک نماد، شش مرتبه تغییر فاز می دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد ٦ مرتبه تغییر فاز خواهد داد.

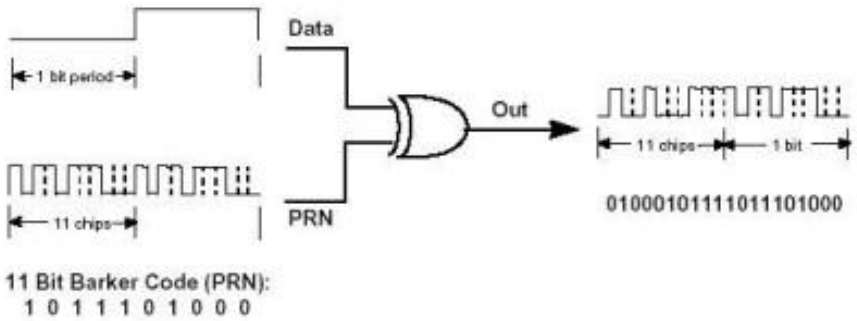
CODE LENGTH (N)	BARKER SEQUENCE
1	+
2	+ + or + -
3	+ + -
4	+ + + - or + + - +
5	+ + + - +
7	+ + + - - + -
11	+ + + - - - + - - + -
13	+ + + + + - - + + - + - +

شکل ۲.۱۱: کدهای بارکر

www.takbook.com

www.takbook.com

لازم به یادآوری است که کاهش پیچیدگی سیستم ناشی از تکنیک تسهیم تفاضلی DPSK به قیمت افزایش نرخ خطای بیتی به ازاء یک نرخ سیگنال به نویز ثابت و مشخص است.

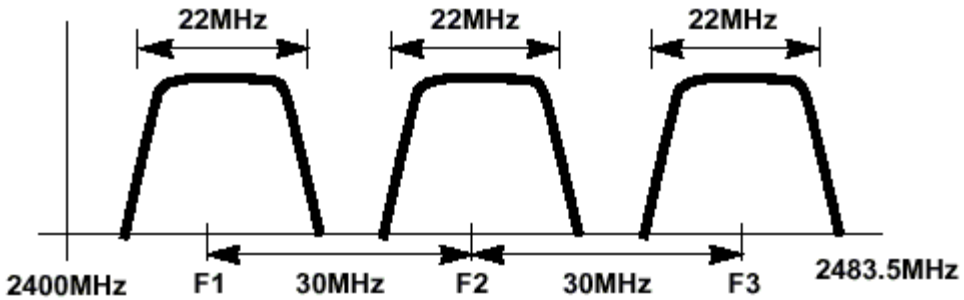


شکل ۲.۱۲ : مدار مدولاسیون با استفاده از کدهای بارکر

شکل ۲.۱۲ مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می دهد.

یکی از نکات مهم در طراحی شبکه های بی سیم، طراحی شبکه سلولی به گونه ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل ۲-۸ سه کانال DSSS در محدوده فرکانسی ISM را نشان می دهد.

۲-۵-۱-٤ استفاده مجدد از فرکانس

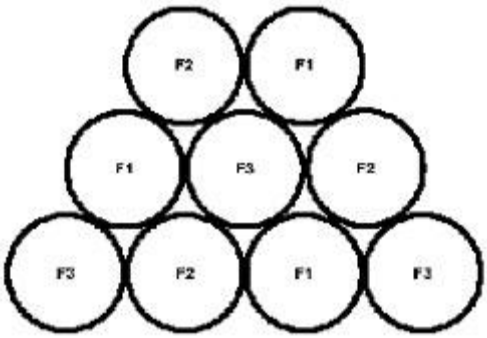


شکل ۲.۱۲ :سه کانال فرکانسی F3,F2,F1

شکل ۲.۱۳مفهوم استفاده مجدد از فرکانس با استفاده از شبکه های مجاور فرکانسی را نشان می دهد. در این شکل مشاهده می شود که با استفاده از یک طراحی شبکه سلولی خاص، تنها با استفاده از سه فرکانس متمایز F1, F2, F3 امکان استفاده مجدد از فرکانس فراهم شده است.

www.takbook.com

www.takbook.com



شکل ۲.۱۳ :طراحی شبکه سلولی

در این طراحی به هر یک از سلول های همسایه یک کانال متفاوت اختصاص داده شده است و بـه ایـن ترتیب تداخل فرکانسی بین سلول های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است کـه در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می رود. نکته جالب دیگر آن است که این شـبکه سـلولی به راحتی قابل گسترش است. خوانندگان علاقمند می توانند دایـره هـای جدیـد را در چهـار جهـت شـبکه سلولی شکل فوق با فرکانس های متمایز F1 ,F2 ,F3 ترسیم و گسترش دهند.

۲-۵-۱-۵ آنتن ها

در یکی تقسیم بندی کلی آنتن های مورد استفاده در استاندارد IEEE 802.11 به دو دسته: تمام جهـت و نقطه به نقطه تقسیم می شوند. واضح است که آنتن های تمام جهته با توجه به آنکه نیازی به تنظیم ندارنـد، راحت تر مورد استفاده قرار می گیرند. این آنتن ها در اغلب کارت های شبکه (کارت های دسترسی) و نیـز نقاط دسترسی یا ایستگاه های پایه بکار می روند.

این آنتن ها در فواصل کوتاه قابل استفاده هستند و برای بهره گیری در فواصـل طـولانی تـر بـه تقویـت کننده های خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت کننده های خارجی میسر و یـا قانونی نیست. از سوی دیگر آنتن های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می شوند و بـه تنظیم دقیق نیاز دارند. محدوده عملیاتی رایج در آنتن های تمام جهته ٤٥ متر و محدوده عملیاتی آنتن هـای نقطه به نقطه و توان بالا در حدود ٤٠ کیلومتر است. در کاربردهایی که اسـتفاده از تقویـت کننـده بـلا مـانع است، این محدوده عملیاتی به شکل قابل توجهی افزایش یافته و تنها توسط خط دید (مسـیر دیـد) محـدود می شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر IEEE 802.11 را تحـت تـأثیر قـرار می دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این استاندارد سعی می کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز بـه سرعت های پایین تر برگردند.

www.takbook.com

www.takbook.com

۲-۶ استاندارد 802.11b

همزمان با برپایی استاندارد IEEE 802.11b یا به اختصار .b۱۱ در سال ۱۹۹۹، انجمن مهندسین برق و الکترونیک تحول قابل توجهی در شبکه سازی های رایج و مبتنی بر اترنت ارائه کرد. این استاندارد در زیر لایه دسترسی به رسانه از پروتکل CSMA/CA سود می برد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است:

۱. استفاده از تکنیک رادیویی DSSS در باند فرکانسی GHz۲.٤ به همراه روش مدولاسیون CCK

۲. استفاده از تکنیک رادیویی FHSS در باندفرکانسی GHz ۲.٤ به همراه روش مدولاسیون CCK

۳. استفاده از امواج رادیویی مادون قرمز

در استاندار ۸۰۲.۱۱ اولیه نرخ های ارسال داده ۱ و ۲ مگابیت در ثانیه است. در حالی که در استاندارد b۸۰۲.۱۱ با استفاده از تکنیک CCK و روش تسهیم QPSK نرخ ارسال داده به ۵.۵ مگابیت در ثانیه افزایش می یابد همچنین با به کارگیری تکنیک DSSS نرخ ارسال داده به ۱۱ مگابیت در ثانیه می رسد.

به طور سنتی این استاندادر از دو فناوری DSSS یا FHSS استفاده می کند. هر دو روش فوق برای ارسال داده با نرخ های ۱ و ۲ مگابیت در ثانیه مفید هستند. جدول ۲.۲ سرعت مختلف قابل دسترسی در این استاندارد را نشان می دهد.

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Seq.)	QPSK	1 MSps	2
5.5 Mbps	8 CCK	QPSK	1.375 MSps	4
11 Mbps	8 CCK	QPSK	1.375 MSps	8

جدول ۲.۲: نرخ های ارسال داده در استاندارد b ۸۰۲.۱۱

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخابره و ارسال فرکانس های رادیویی را کنترل می کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده ۲.٤GHz تا ۲.٤۸۳۵ GHz برای فناوری های رادیویی استاندارد IEEE 802.11b اختصاص داده است.

www.takbook.com

www.takbook.com

۲-٦-۱ اثرات فاصله

فاصله از فرستنده برروی کارایی و گذردهی شبکه های بیسیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد ۸۰۲.۱۱ با توجه به نرخ ارسال داده تغییر می کند و به طور مشخص در پهنای باند Mbps ۱۱ این فاصله ۳۰ تا ٤٥ متر و در پهنای باندMbps ۵.۵ این فاصله ٤۰ تا ٤٥ متر و در پهنای باندMbps ۲ این فاصله ۷۵ تا ۱۰۷ متر است. لازم به یادآوری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرند و شرایط فیزیکی و محیطی تغییر می کنند.

در استاندارد b ۸۰۲.۱۱ پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می نماید توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل TCP اتفاق می افتد) عمل می کند. در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می کند که بسته از دست رفته است و مجددا آن بسته را ارسال می کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می یابد (Fall Back) تا در نهایت به مقدار ۱ Mpbs برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته ای را برای آن گیرنده ارسال نمی کند. به این ترتیب فاصله نقش مهمی در کارایی (میزان بهره وری از شبکه) و گذردهی (تعداد بسته های غیرتکراری ارسال شده در واحد زمان) ایفا می کند.

۲-٦-۲ پل بین شبکه ای

بر خلاف انتظار بسیاری از کارشناسان شبکه های کامپیوتری، پل بین شبکه ای یا Bridging در استاندارد b۸۰۲.۱۱ پوشش داده نشده است. در پل بین شبکه ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط یک شبکه محلی با یک یا چند شبکه محلی دیگر فراهم می شود. این کاربرد به خصوص در مواردی که بخواهیم بدون صرف هزینه کابل کشی (فیبر نوری یا سیم مسی) شبکه محلی دو ساختمان را به یکدیگر متصل کنیم بسیار جذاب و مورد نیاز می باشد. با وجود اینکه استاندارد b۸۰۲.۱۱ این کاربرد را پوشش نمی دهد ولی بسیاری از شرکت ها پیاده سازی های انحصاری از پل بیسیم را به صورت گسترش و توسعه استاندارد b۸۰۲.۱۱ ارائه کرده اند. پل های بیسیم نیز توسط مقررات FCC کنترل می شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ٤ وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال های ساطع شده در شبکه های محلی نیز نباید از ۱ وات تجاوز نماید.

www.takbook.com

www.takbook.com

۲-۷ استاندارد 802.11a

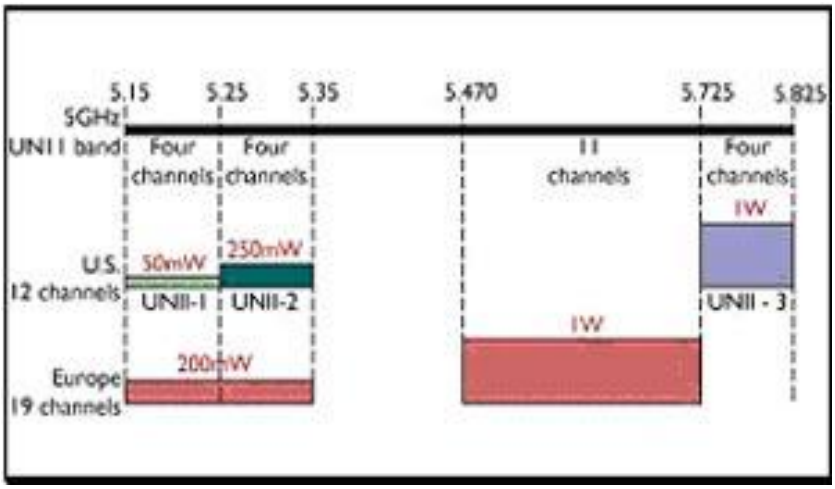
استاندارد 802.11a ، از باند رادیویی جدیدی برای شبکه های محلی بیسیم استفاده می کند و پهنای باند شبکه های بیسیم را تا ٥٤ Mbps افزایش می دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیونی موسوم به OFDM است. نرخ های ارسال داده در استاندارد IEEE 802.11a عبارتند از:٦,٩,١٢,١٨,٢٤,٣٦,٤٨,٥٤ Mbps که بر اساس استاندارد، پشتیبانی از سرعت های ٦,١٢,٢٤ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه های محلی بیسیم، استاندارد IEEE 802.11a را نسل آینده IEEE 802.11 تلقی می کنند و حتی برخی از محصولات مانند تراشه های Atheros وکارت های شبکه PCMCIA/Cardbus محصول Card Access Inc. استاندارد IEEE 802.11a را پیاده سازی کرده اند. بدون شک این پهنای باند وسیع و نرخ داده سریع محدودیت هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد IEEE 802.11a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE 802.11/b کاهش یابد. علاوه بر آن به سبب افزایش سربارهای پردازشی در پروتکل، تداخل، و تصحیح خطاها، پهنای باند واقعی به مراتب کمتر از پهنای باند اسمی این استاندارد است. همچنین در بسیاری از کاربردها امکان سنجی و حتی نصب تجهیزات اضافی نیز مورد نیاز است که به تبع آن موجب افزایش قیمت زیرساختار شبکه بیسیم می شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد IEEE 802.11b بوده و به همین خاطر به نقاط دسترسی یا ایستگاه پایه بیشتری نیاز خواهیم داشت که افزایش هزینه زیرساختار را به دنبال دارد. این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می شود:

UNII-1 @ 5.2 GHz
UNII-2 @ 5.7 GHz
UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمینهاستانداردهای ۸۰۲.۱۱ این باور است که a ۸۰۲.۱۱ قبل از b ۸۰۲.۱۱ مورد بهره برداری واقع شده است. در حقیقت b ۸۰۲.۱۱ نسل دوم استانداردهای بیسیم (پس از ۸۰۲.۱۱)است و a ۸۰۲.۱۱ نسل سوم از این مجموعه استاندارد به شمار می رود. استاندارد a۸۰۲.۱۱ برخلاف ادعای بسیاری از فروشندگان تجهیزات بیسیم نمی تواند جایگزین b ۸۰۲.۱۱شود زیرا لایه فیزیکی مورد استفاده در هریک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هریک متفاوت است.

www.takbook.com

www.takbook.com



شکل ۲.۱٤ : تخصیص باند فرکانسی در UNII

در شکل ٤-۱ این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می شود. این سه ناحیه کاری ۱۲ کانال فرکانسی را فراهم می کنند. باند UNII-1 برای کاربردهای فضای بسته، باند UNII-2 برای کاربردهای فضای بسته و باز، و باند UNII-3 برای کاربردهای فضای باز و پل بین شبکه ای به کار برده می شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قاره اروپا قابل استفاده نیست. در اروپا HyperLAN2 برای شبکه های بیسیم مورد استفاده قرار می گیرد که به طور مشابه از باند فرکانسی a۸۰۲.۱۱ استفاده می کند. یکی از نکات جالب توجه در استاندارد a۸۰۲.۱۱ تعریف کاربردهای پل سازی شبکه ای در کاربردهای داخلی و فضای باز است. در واقع این استاندارد مقررات لازم برای پل سازی و ارتباط بین شبکهای از طریق پل را در کاربردهای داخلی و فضای باز فراهم می نماید. در یکی تقسیم بندی کلی می توان ویژگی ها و مزایای a۸۰۲.۱۱ را در سه محور زیر خلاصه نمود.

افزایش در پهنای باند در مقایسه با استاندارد b۸۰۲.۱۱ (در استاندارد a۸۰۲.۱۱ حداکثر پهنای باند ٥٤ Mbps) می باشد.

استفاده از طیف فرکانسی خلوت (باند فرکانسی ٥ GHz)

استفاده از ۱۲ کانال فرکانسی غیرپوشا (سه محدوده فرکانسی که در هریک ٤ کانال غیرپوشا وجود دارد)

www.takbook.com

www.takbook.com

۲-۸ استاندارد بعدی IEEE 802.11g

این استاندارد مشابه IEEE 802.11b از باند فرکانسی GHz ۲.٤ (یا طیف ISM) استفاده می کند و از تکنیک OFDM به عنوان روش مدولاسیون بهره می برد. البته PBCC نیز یکی از روش های جایگزین و تحت بررسی برای انتخاب تکنیک مدولاسیون در این استاندارد به شمار می رود. ۸۰۲.۱۱ g از نظر فرکانسی، تعداد کانال های غیرپوشا، و توان مشابه ۸۰۲.۱۱ b است. محدوده های عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تا حدودی این محدوده عملیاتی را کاهش می دهد. پهنای باند ٥٤ Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می رود. یکی دیگر از مزایای جالب توجه ۸۰۲.۱۱ gسازگاری با ۸۰۲.۱۱b است. در نتیجه ارتقاء از تجهیزات ۸۰۲.۱۱ b به استاندارد جدید ۸۰۲.۱۱ gامری سر راست خواهد بود. جدول۲.۳سه استاندارد شبکه های بیسیم را با یکدیگر مقایسه می کند.

	IEEE802.11b	IEEE802.11a	IEEE802.11g
کاربرد های احتمالی	-جایگزین شبکه های بی سیم -فراهم آوردن تحرک و سیار بودن کاربران -شبکه سازی در محل هایی که استفاده از سیم امکان پذیر نمی باشد پل سازی بین شبکه های محلی دور فواصل دور(٤٠ کیلومتر)	-جایگزین شبکه های بی سیم -فراهم کننده پهنای باند زیاد در کابرد های صدا و توصیر و نظایر آن -شبکه سازی در محل هایی که استفاده از سیم امکان پذیر نمی باشد	-ارتقای شبکه های ۸۰۲.۱۱bو رقیبی برای ۸۰۲.۱۱a -کارایی مشابه با ۸۰۲.۱۱ a در فواصل طولانی
مزایا	-استاندارد رایج وتکامل یافته -قیمت منطقی =گذر دهی قابل قبول در فواصل زیاد (نرخ ارسال)	-گذر دهی بالا در فواصل کم -افزایش تعداد کانال های فرکانسی غیر پوشا -تداخل فرکانسی کمتر	-سازگاری با ۸۰۲.۱۱ b -محدوده عملیاتی زیاد (نظیر ۸۰۲.۱۱b) -گذر دهی(نرخ ارسال) بیشتر
معایب	-دارا بودن کمترین گذر دهی(نرخ ارسال) در مقایسه با سایر فناوری های بی سیم -استفاده از تنها سه کانال فرکانسی غیرپوشا	-فناوری نسبتا گران -ناسازگاری با ۸۰۲.۱۱ b -محدوده عملیاتی کوچک -محدودیت های FFC (حداکثر توان)بر روی آنتن ها در هر باند فرکانسی	-عدم وجود محصول فراگیر -محدودیت های کانال فرکانسی نظیر b ۸۰۲.۱۱(ه کانال غیر پوشا)

جدول ۲.۳ : مقایسه استانداردهای بیسیم IEEE 802.11

www.takbook.com

www.takbook.com

۳ فصل سوم :مفاهیم امنیتی در شبکه های بی سیم

Chapter three:Security Concepts in Wi-Fi

مراجع:[9]

www.takbook.com

www.takbook.com

۳-۱ فاکتور های امنیتی در شبکه های بی سیم

فاکتور هایی که امنیت در شبکه ها بی سیم را تعریف می کند به پنج مفهوم کلی دسته بندی می شود که عبارتست از :

۱.سارقان(thefts):سارقان کاربران غیر مجاری هستند که قصد نفوذ و ورود به شبکه را دارند تا داده ها واطلاعات مهم را برای اهداف خاص سرقت کنند .اهداف این سارقان متفاوت است و از افراد مهاجم خارجی می تواند باشد تا کارمندان داخلی سازمان،بنابراین باید یک تدبیر امنیتی در نظر گرفت تا از ورود این افراد به سیستم جلوگیری شود.

۲.کنترل دسترسی(Access control):بسیاری از سازمان ها یک سری از مجوز های دسترسی بسیار ساده ای دارند و این می توان از هر چیزی خطرناک تر باشد به خصوص در یک شبکه محلی بی سیم که به راحتی می توان نفوذ کرد،در نتیجه روال های کنترل دسترسی سیستم هایی که در شبکه های بی سیم استفاده می شوند، باید حتما اعمال شود و به انداز های قوی باشد که از ورود افراد مهاجم و خارجی و حتی ویروس ها ،به شبکه جلوگیری کند.

۳.احراز هویت(Authentication):آیا شما مطمئن هستید کاربری که از قصد استفاده از سیستم را دارد واقعا همان شخصی است که ادعا می کند؟متاسفانه یک امر رایج در شبکه ای بی سیم این است که افراد از اکانت های یک دیگر برای استفاده از شبکه استفاده می کنند و این بهترین فرصت برای مهاجمان برای ورود به شبکه می باشد،برای جلوگیری از ورود این افراد به شبکه، باید تنظیمات روتر را طوری انجام دهید که تنها اتصالات از طریق کارت شبکه های مجاز احرازهویت شده را قبول کند،همانطور که می دانیم هر کارت شبکه دارای یک آدرس مک منحصر به فرد می باشد،و برای افزایش امنیت می توانیم تنها اتصالات از کارت شبکه هایی را قبول کنیم که از قبل در روتر شناسایی شده باشند.

٤.رمز نگاری(Encryption):اگر مهاجم به طور مستقیم نتواند به شبکه دسترسی پیدا کند و نفوذ کند می تواند از طریق شنود ترافیک وبسته های شبکه،به شبکه حمله کند و این بدین معنی است که مهاجمی که نتوانسته به طور مستقیم به شبکه نفوذ کند قادر است از طریق دیگری به اطلاعات مهم دسترسی پیدا کند و انها را سرقت کند و حتی می تواند از طریق شنود بسته های انتقالی اطلاعات حساس شما مثل نام کاربری و کلمه عبور را شنود کنده و بدین ترتیب دوباره به شکل مستقیم در سیستم نفوذ کند.

روتر های بی سیم سطوح مختلفی از رمزنگاری را پشتیبانی می کنند،متاسفانه اکثر مدیران شبکه این امکانات در روتر را فعال نمی کنند.

www.takbook.com

www.takbook.com

امنیت معادل سیمی(WEP[۵]) پروتکل امنیتی است که توسط استاندارد IEEE802.11 برای استفاده در شیکه های بی سیم ،تعریف شده است.WEP سطوح مختلف امنیتی معادل با یک شبکه سیمی را ارائه می دهد،این پروتکل در هر دو لایه فیزیکی و پیوند داده مورد استفاده قرار می گیرد و امنیت نقطه به نقطه را فراهم نمی کند.

بیشتر روتر ها بی سیم رمزنگاری ٦٤ بیت و ١٢٨ بیتی را پشتیبانی می کنند و ازیک کلید رمزنگاری از پیش تعیین شده برای عملیات رمز نگاری استفاده می کنند که در طرف مقابل از این کلید برای رمز گشایی استفاده می شود.

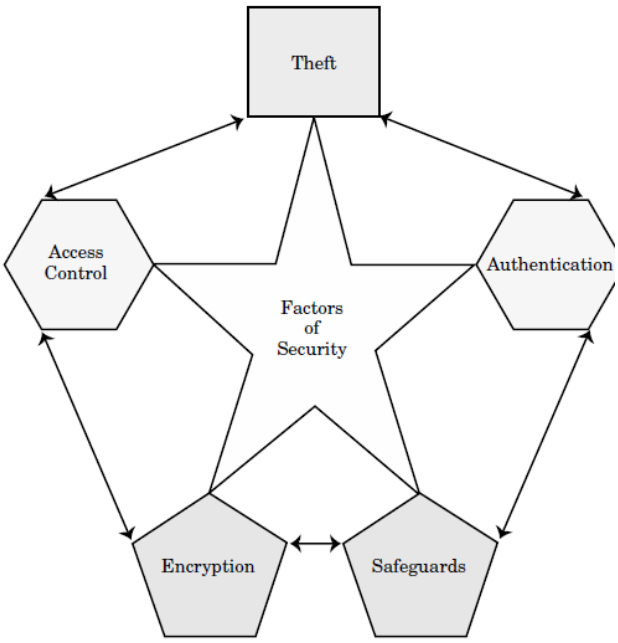
۵.محافظت های امنیتی (Safeguards):برای اعمال روش های محافظتی در شبکه های بی سیم، در مرحله اول باید شبکه بی سیم مورد نظر را کاملا شناخت،سپس باید تنظیمات امنیتی روتر را پیکر بندی نمود و از کلید های حداقل با طول ٦٤ بیت استفاده نمود ،البته باید این نکته را توجه داشت که بعضی از کارت های شبکه بی سیم فقط سطوح خاصی امنیتی را پشتیبانی می کنند.

بعد از اعمال تنظیمات امیتی روتر می توان روش های دیگر برای افزایش امنیت شبکه استفاده نمود ،مثلا از روش هایی استفاده نمود که بلافاصله بعد از هک شدن شبکه مطلع شویم تا از خرابکاری بیشتر جلوگیری کنیم ،مثلا روتر ها دارای امکانی هستند که جریان ترافک را درشبکه نشان می دهند و نرم افزار های مختلفی وجود دارند که می توانند که از این اطلاعات برای تحلیل ترافیک استفاده کنند ،پس ما می توانیم از این نرم افزار ها برای مدیریت و نظارت بهتر شبکه استفاده کنیم و مثلا اگر حجم نامعقولی از ترافیک را متوجه شدیم سریعا حجم تفکیکی به ازای هر اتصال را بررسی کنیم و با ردگیری ترافیکی به منشا آن برسیم و سریعتر برای جلوگیری از کار افتادن شبکه ،اقدام کنیم.

[۵] *Wired equivalent privacy*

www.takbook.com

www.takbook.com



شکل ۳.۱:فاکتور های امنیتی در شبکه های بی سیم

۳-۲ سیستم تشخیص نفوذ:

تعداد زیادی از نرم افزار های تجاری وجود دارد که از تکنیک نقش – مبنا(Role-Based) ،به طور اتوماتیک برای تشخیص نفوذ به سیستم استفاده می کنند،سیستم تشخیص نفوذ تمام فعالیت های به –داخل وبه–خارج شبکه را بررسی می کند تا حمله از سوی مهاجمی را که قصد دارد به شکل غیر مجاز به سیستم وارد شود را، شناسایی کند.

انواع مختلف روش های تشخیص نفوذ عبارتست از:

۱.شناسایی الگو(Pattern detection): در این تکنیک که معمولاًبا نام تشخیص مبتنی بر امضاء شناخته شده است، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می‌شوند. به طوری که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می‌شود. در این روش‌ها، معمولاً تشخیص دهنده دارای پایگاه داده‌ای از امضاءها یا الگوهای حمله است و سعی می‌کند با بررسی ترافیک شبکه، الگوهای مشابه با آن چه را که در پایگاه داده‌ٔ خود نگهداری می‌کند، بیابد. این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته شده می‌باشند و در صورت بروز حملات جدید در سطح شبکه، نمی‌توانند آن‌ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سامانه تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن‌ها عیناً به سیستم داده شده‌است.

www.takbook.com

www.takbook.com

روش دیگری هم وجود دارد که می تواند زیر دسته این روش قرار بگیر و عبارتست از روش تشخیص رفتار غیرعادی،در این روش، یک نما از رفتار عادی ایجاد می‌شود. یک ناهنجاری ممکن است نشان دهنده یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه های عصبی، تکنیک های یادگیری ماشین و حتی سیستم های ایمنی زیستی استفاده می‌شود. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن ها پیدا کرد. رفتارهایی که از این الگوها پیروی می‌کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می‌شود. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می‌پیوندد، غیرعادی فرض می‌شود.

۲.سامانه تشخیص نفوذ مبتنی بر میزبان وشبکه(NIDS[۶],HIDS[۷]): سیستم مبتنی بر میزبان، شناسایی و تشخیص فعالیت‌های غیرمجاز بر روی رایانه میزبان را بر عهده دارد. سامانه تشخیص نفوذ مبتنی بر میزبان می‌تواند حملات و تهدیداتی را روی سیستم های بحرانی تشخیص دهد (شامل دسترسی به فایل ها، اسب های تروا و ...) که توسط سامانه های تشخیص نفوذ مبتنی بر شبکه قابل تشخیص نیستند. HIDS فقط از میزبان هایی که روی آن ها مستقر است محافظت می‌کند و کارت واسط شبکه (NIC) آن ها به صورت پیش فرض در حالت باقاعده کار می‌کند. حالت باقاعده در بعضی از موارد می‌تواند مفید باشد چون همه کارت‌های واسط شبکه قابلیت حالت بی قاعده را ندارند.HIDS به واسطه مکان شان روی میزبانی که باید نظارت شود، از همه انواع اطلاعات محلی اضافی با پیاده‌سازی‌های امنیتی (شامل فراخوانی‌های سیستمی، تغییرات فایل های سیستمی و اتصالات سیستم) مطلع می‌باشند. این مساله هنگام ترکیب با ارتباطات شبکه‌ای، داده‌های خوبی را برای جستجوی رویدادهای ممکن فراهم می‌کند.

شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستمهای بحرانی، به عهده سامانه تشخیص نفوذ مبتنی بر شبکه است. NIDS، به عنوان دومین نوع IDSها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌گیرد می‌پردازند. به عبارت دیگر معیار NIDS ، تنها بسته‌هایی است که بر روی شبکه‌ها رد و بدل می‌گردد. از آن جایی که NIDS تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گستردگی بیش تری داشته و فرایند تشخیص را به صورت توزیع شده انجام می‌دهند. با این وجود این سیستم ها در رویایی با بسته‌های رمزشده و یا شبکه‌هایی با سرعت و ترافیک بالاکارایی خود را از دست می‌دهند.

---

[۶] *Network-based intrusion detection system*

[۷] *host-based intrusion detection system*

www.takbook.com

www.takbook.com

۳.پاسخ فعال و غیر فعال در سیستم تشخیص نفوذ:در پاسخ فعال، IDSها، به مدیر امنیتی سیستم اطلاعاتی دربارهحمله توسط تلفن همراه، نامهالکترونیکی، پیام روی صفحهرایانه یا پیامی برای کنسول SNMP می‌دهند. این اطلاعات شامل : آدرس IP منبع حمله

، آدرس IP مقصد حمله، نتیجه حمله، ابزار یا مکانیزم‌های مورد استفاده برای مهار حملهو گزارش‌ها و اتصال‌ها حمله‌های سیستم و رویدادهای مربوطه باشد.

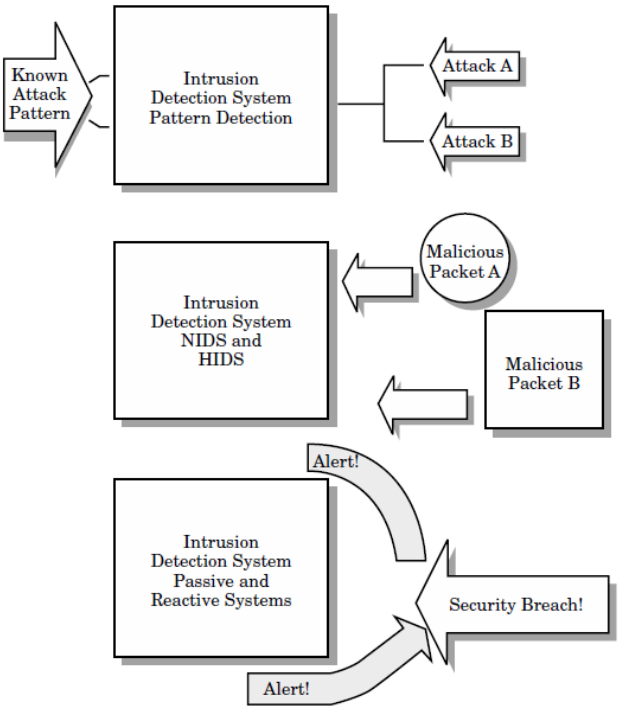
در پاسخ فعال سامانه‌های تشخیص نفوذ از لحظه‌ای که به کار می‌افتند، ضمن به دست آوردن اطلاعات مربوط به رخدادها و تجزیه و تحلیل آن‌ها، اگر نشان‌هایی دال بر وقوع یک حمله را تشخیص دهند، پاسخ لازم را در قبال آن به نحوه های مختلف تولید می‌کنند. گاهی این پاسخ به صورت یک هشدار به مدیر شبکه است و گاهی نوشتن یک اطلاع در فایل رخدادها و یا به صورت تنظیم مجدد دیواره آتش و یا دستگاه‌های دیگری در شبکه‌است. IDSهای فعال هر نفوذی را که تشخیص دهد به طور خودکار پاسخ می‌دهند و خود به سه دسته تقسیم می‌شوند:

الف: پاسخ فعال براساس جمع‌آوری اطلاعات اضافی

ب: پاسخ فعال از نوع تغییر محیط

ج: پاسخ فعال از نوع عکس العمل در مقابل حمله

نمایی کلی از روش های سیستم نفوذ در شکل ۳.۲ نمایش داده شده است



شکل ۳.۲:روش های تشخیص نفوذ

www.takbook.com

www.takbook.com

۳-۳ چالش های امنیتی در شبکه های WI-Fi

مطمئا یکی از بزرگترین نگرانی ها، بعد از راه اندازی و پیکر بندی شبکه های بی سیم ،برقراری امنیت می باشد،با توجه به این که محیط بی سیم محیطی نا امنی محسوب می شود و هر لحظه می تواند مورد حمله قرار گیرد و اطلاعات و داده های شبکه سرقت شود،برقرای امنیت یکی از بزرگترین چالش ها در این شبکه ها می باشد.

انواع تهدید هایی که ممکن است امنیت در شبکه ای بی سیم را به خطر اندازد عبارتند از:

۱.افشای اطلاعات:هرگونه دسترسی غیر مجاز به اطلاعات و داده های شبکه که گاهی می تواند اطلاعات حیاتی و مهم مثل اطلاعات نظامی یا اطاعات حساب بانکی افراد باشد.

۲.دسترسی های غیر مجاز:هر گونه دسترسی به اطلاعات و داده ها و نفوذ به شبکه توسط افراد غیر مجاز و احراز هویت نشده به سیستم،دسترسی غیر مجاز نام دارد.

۳.منع سرویس(DOS[۸]): هر گونه عملیات خرابکارانه که منجر به این شود که سرویس دهی سیستم مختل شود ،حملات منع سرویس گفته می شود.در چند سال اخیر این حمله یکی از مهمترین حملات به شمار می رود که در ان حمله کننده با اعمال بار زیاد به شبکه باعث مختل شدن کار شبکه می ش.د.

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی 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، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است

– تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود

[۸] Denial Of Service

www.takbook.com

www.takbook.com

ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.

– نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.

– اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.

– حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.

– نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.

– با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.

– کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

– یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.

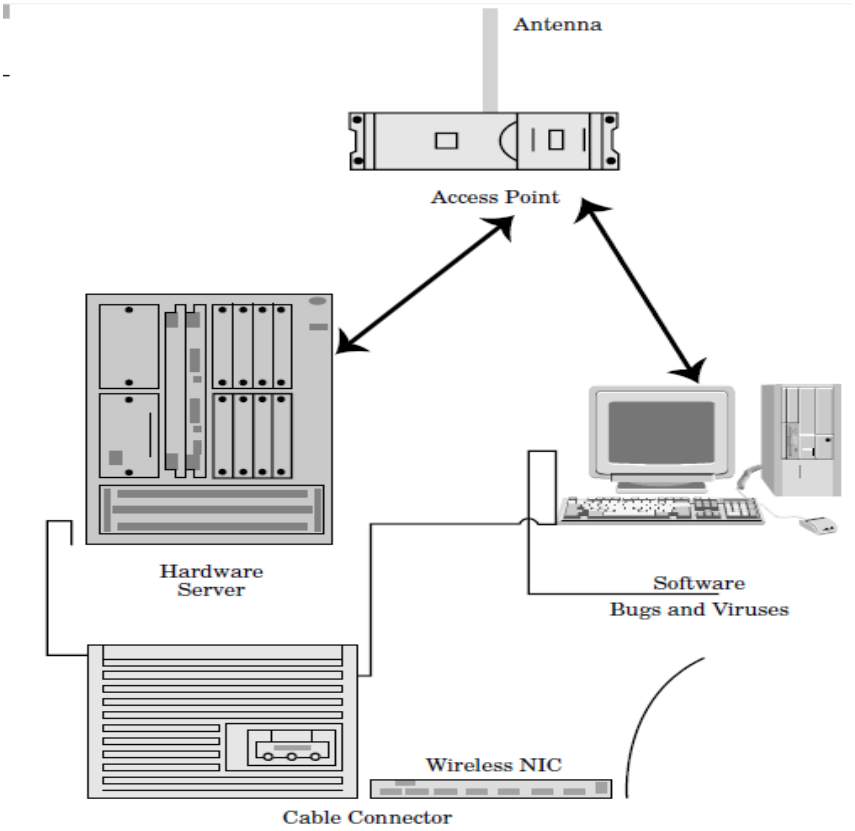
– در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد شبکه نیز وجود دارد.

۳-٤ نقاط آسیب پذیر و قابل نفوذ در شبکه های Wi-Fi

به طور کلی چندین نقطه آسیب پذیر در شبکه های بی سیم وجو دارد و در صورتی که مهاجمین از این نقاط اطلاعات به دست اورند به راحتی می توانند به شبکه نفوذ کرده و زیر ساخت شبکه را به هم بریزند،این نقاط در شکل ۳.۳ نمایش داده شده است.

www.takbook.com

www.takbook.com



شکل ۳.۳ نقاط حساس در شبکه های بی سیم

این نقاط عبارتست از :

۱.نقطه دسترسی

۲.آنتن

۳.کارت های شبکه بی سیم

٤.کابل های اتصال

۵..سرور سخت افزاری

٦.باگ های نرم افزاری و ویروس ها

این امکان وجو دارد که از هر کجا به سیستم نرم افزاری نفوذ کرد ،هر چند که firmware های کاملا مناسب در نقاط دسترسی و روتر ها نصب شده باشد،در حقیقت firmware ها در این وسایل نرم افزار هایی هستند که ویژگی ها و قابلیت هایی را از جمله قابلیت های امنیتی را به ارمغان می آورند،اما باید توجه داشت که اگر هکر ها بتوانند به تجهیزات و وسایل دسترسی پیدا کنند به راحتی می توانند firmware و نرم افزار های جدید را بر روی این تجهیزات قرار دهند تا مطابق خواسته ی آنها عمل کنند یا حتی این نرم افزار ها دستکاری کرده تا نتوانند وظایف امنیتی خود را به درستی انجام دهند.

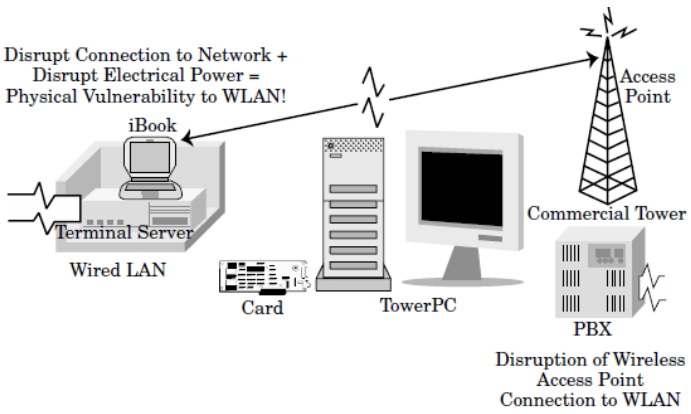
www.takbook.com

www.takbook.com

سرور ها و نرم افزار ها می توانند توسط ویروس ها مورد حمله قرار بگیرند،اکثر ویروس های جدید اتصالات آداپتور شبکه را شناسایی می کنند و ارتباطات را در شبکه به هم می ریزند،اساسا این ویروس ها با اهداف خاموش کردن کامل تجهیزات شبکه های بی سیم و خراب کردن سیگنال و رساندن گذدر دهی سیگنال در حد صفر می باشد.خاموش کردن تجهیرات شبکه مثل نقاط دسترسی یا روتر ها می توانند کل شبکه را مختل کند واز کار بیاندازد،نکته قابل توجه در این حملات سخت بودن شناسایی حمله و شناسایی این که دلیل خرابی سخت افزاری یا نرم افرای بوده،می باشد.

- هر گونه دست کاری و مختل کردن و از کار انداختن، در شبکه های بی سیم می تواند به صورت زیر باشد:
- بر هم زدن ارتباطات بین نقاط دسترسی
- قطع کردن اتصال اساسی شبکه بی سیم به شبکه سیمی
- ایزوله کردن و جدا سازی چندین نقطه دسترسی برای این که نتوانند با سایر نقاط دسترسی ارتباط برقرار کنند ،که می تواند منجر به کار افتادن شبکه های بی سیم شود.
- خاموش کردن و قطع برق یک یا چند نقطه دسترسی

این روش ها در شکل ۳.٤ نمایش داده شده است.در مجموع باید گفت که برای یک هکر خیلی ساده می باشد که از یک کارت شبکه بی سیم که قبلا در شبکه شناخته شده است ومجاز شماری شده استفاده کند و به شبکه حمله کند و درنتیجه بر هم زدن اتصالات در نقاط دسترسی ،منابع شبکه ،سرور ،منبع برق و قطع کردن ارتباط با شبکه سیمی سبب از کار افتادن و کاهش کارایی و خراب شدن شبکه شود.



شکل ۳.٤ :تهدیدات فیزیکی در شبکه بی سیم

www.takbook.com

www.takbook.com

۳-۵ امن سازی شبکه های بی سیم

در مجموع برای امن سازی شبکه های بی سیم باید از امکانات امنیتی ادغام شده در استاندارد ۸۰۲.۱۱ استفاده نمود،در حقیقت این استاندارد امکانات و ویژگی هایی را فراهم می آورد که باعث افزایش میزان امنیت در یک شبکه می شود.به طور کلی ابتدا برای این که بتوان به امنیت در این شبکه ها رسید باید ویژگی های زیر را اعمال کرد که در پروتکلWEP برای برقرای امنیت در شبکه های بی سیم استفاده شده است:

۱.احراز هویت:یکی از اهداف پروتکل WEP که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار گرفته است،کنترل دسترسی و احراز هویت در شبکه های بی سیم می باشد.

۲.ایمنی(Privacy):WEP سطح کنترل زیادی در هنگام برقراری در ارتباطات بی سیم فراهم می آورد و جلوی هر گونه تغییر و استراق سمع در داده های ارتباطی را می گیرد و به عبارت دیگر برای این به کار می رود که به شما این اطمینان را بدهد که داده های دریافت شده از یک منبع مورد اعتماد است و هرگونه تغییر و دست کاری در آن رخ نداده است.

۳-۵-۱ احراز هویت

وقتی یک کاربر شبکه بی سیم سعی می کند که به زیر ساخت شبکه سیمی وصل شود، دو رویکرد را می توان درباره ی این در خواست اعمال کرد:

۱.سیستم های باز:هر کاربری که در محدوه رادیویی نقطه دسترسی باشد به راحتی می تواند به شبکه وصل شود و هیچ گونه محدودیتی در رابطه با وصل شدن کارت های شبکه اعمال نمی کند.

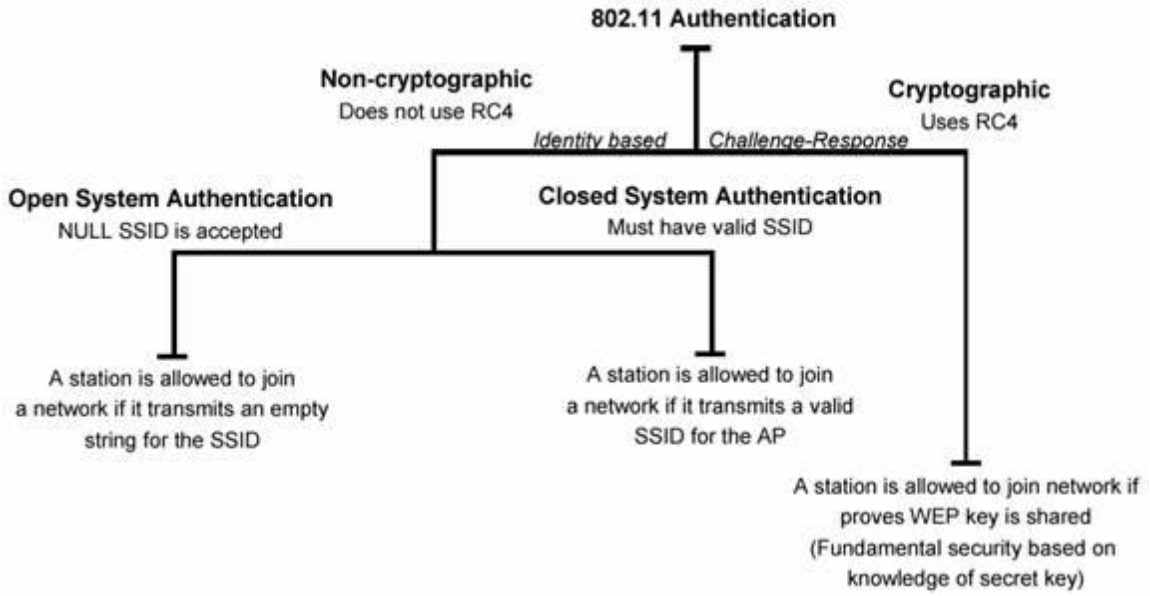
۲.سیستم رمز شده (بسته):در این سیستم داده ها با استفاده از الگوریتم RC4 رمز می شود و هکر ها نمی توانند به داده های در حال جریان در شبکه دسترسی پیدا کنند.در این سیستم برای این که کاربری به شبکه وصل شود باید به نقطه دسترسی SSID [۹]را ارسال کتد،که در حقیقت یک عدد منحصر به فرد است که تنها کاربران ثبت شده در سیستم می دانند.در این سیستم برای مجاز شمار نیز از رمز نگاری استفاده می شود

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

[۹] service set identifier

www.takbook.com

www.takbook.com



شکل ۳.۵ روش های Authentication در استاندارد 802.11

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.

۳-۵-۱-۱ Authentication بدون رمزنگاری

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت کلاینت وجود دارد. در هر دو روش کلاینت متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک Service Set Identifier (SSID) 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 کلاینت هایی 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.

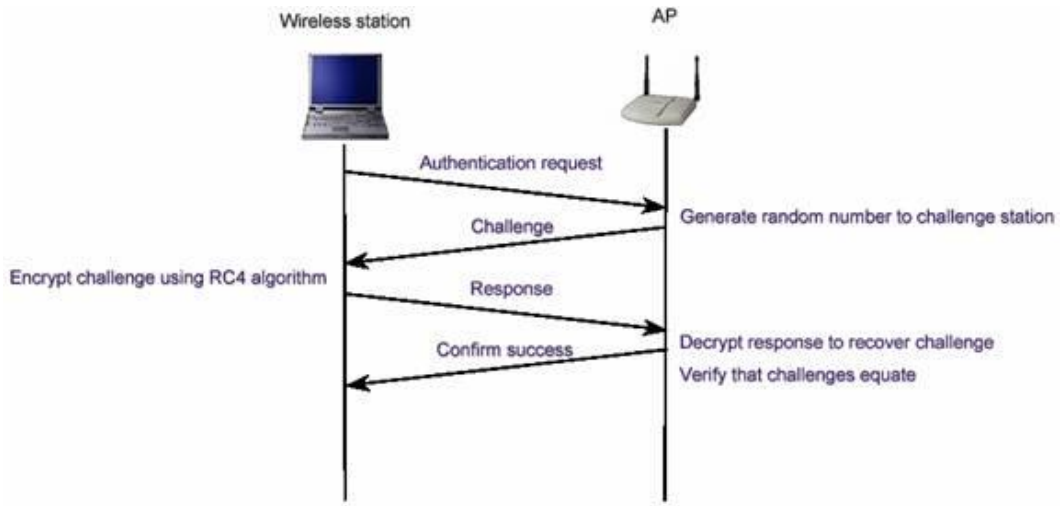
www.takbook.com

www.takbook.com

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 شبکه های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

۳-۵-۱-۲ 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 کلاینت از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد :



شکل ۳.٦ فرایند Authentication با رمزنگاری RC4

در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن‌را به کلاینت می‌فرستد. کلاینت 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

www.takbook.com

www.takbook.com

اینکه کلاینت 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 کلاینت اطمینان حاصل می‌کند. به بیان دیگر کلاینت هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی یی که با آن در حال تبادل داده های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

ب) تمامی روش هایی 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.

۳-۵-۲ امنیت داده ها

استاندارد ۸۰۲.۱۱ از طریق مکانیسم رمزنگاری امنیت در شبکه های بی سیم را تامین می کند.پروتکل WEP در استاندراد ۸۰۲.۱۱ از الگوریتم RC4 با کلید متقارن برای رمز نگاری استفاده می کند.WEP برای تمامی داده ها در شبکه های بی سیم مناسب می باشدو برای حفاظت و امن ساری کانال مورد استفاده قرار می گیرد.این پروتکل از داده ها محافظت می کند زمانی که در حال انتقال از کانال هستند و از پروتکل های زیر استفاده می کنند:

-پروتکل کنترل انتقال (TCP)/پروتکل اینترنت(IP)

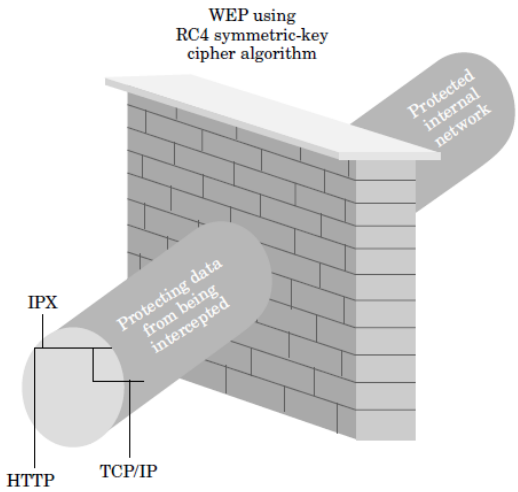
-تبادل بسته های اینترنت(IPX[۱۰])

-پروتکل HTTP

[۱۰] *Internet packet exchange*

www.takbook.com

www.takbook.com



شکل ۳.۷ :محافظت از داده ها در کانال های ارتباطی

WEP برای رمزنگاری با طول کلید بین ٤٠ تا ١٠٤ بیت طراحی شده است و هر چه طول کلید افزایش یابد میزان امنیت در کانال نیز افزایش خواهد یافت،در حقیقت اگر کلید با طول کم انتخاب شود به هکر ها اجازه ی حمله "جست و جوی تمام حالات" داده می شود و می توانند کلید را به دست آورده و اطلاعات را رمز گشایی کنند .متاسفانه تجربه نشان داده است که بسیاری از سازمان ها تنظیمات امنیتی را فعال نمی کنند و اگر هم استفاده کنند از طول کلید کوچک استفاده می کنند که در نهایت منجر به هک شدن شبکه شده است.

٣-٦ مدیریت کلید ها

یکی از چالش های مهم در استاندارد ٨٠٢.١١ مدیریت کلید ها می باشد.مدیران در شبکه های بی سیم در مورد چند مورد در رابطه با کلید ها مسئول می باشند:

١.ایجاد کلید ها

٢.اشتراک کلید بین کاربران شبکه

٣.نگه داری کلید ها به شکلی که دست مهاجمین و هکرها نیافتد

٤.نظارت بر این که هرکسی از چه کلیدی برای عملیات رمزنگاری استفاده می کند

٥.حذف کلید هایی که لو رفته و به صورت اشتراکی استفاده می شود

www.takbook.com

www.takbook.com

اما چه اتفاقی می افتد اگر کسی مسئولیتی در رابطه با مدیریت کلید ها که در بالا ذکر شده است بر عهده نگیرد؟در واقع شبکه شما در برابر حملات هکر ها آسیب پذیر خواهد شد و منجر به موارد زیر خواهد شد:

- کلیدهای WEP یکتا نیستند ومی توانند توسط چندین کاربر استفاده شوند!
- پسورد های پیش فرض که توسط کارخانه تنظیم شده اند تغییر پیدا نمی کند و باعث می شود که به راحتی هکر ها از این پسورد ها مطلع شوند.
- کلید های نا مناسب نه کلید هایی که همه اعداد آن یک یا همه اعداد ان صفر باشند ،بلکه کلید هایی که به راحتی هکر ها می توانند حدس بزنند و در اولین جست وجو به آن خواهند رسید.

۳-۷ صحت داده

یکی دیگر از امکانات امنیتی که استاندارد ۸۰۲.۱۱ فراهم می آورد ،حفظ صحت داده زمانی که در کانال و چندین نقطه دسترسی می گذرد ،می باشد. تکنیکی که استفاده می شود استفاده از کد های CRC می باشد در حقیقت بعد از دریافت بسته و رمز گشایی آن کد CRC بر اساس محتوای بسته محاسبه می شود و با کد CRC که فرستنده در بسته گزاشته است مقایسه می شود،اگر مطابقت کرد یعنی بسته از تغییرات مصون بوده و گرنه متوجه می شویم که بسته در راه دچار تغییرات شده و فاقد اعتبار می باشد.

۳-۸ نتیجه گیری

با توجه به ماهیت محیط شبکه های بی سیم Wi-Fi و در دسترس بودن ابزار های پیشرفته حمله و نفوذ به شبکه توسط هکر ها،برقرای امنیت در شبکه های بی سیم یکی از بزرگترین چالش ها شناخته می شود.در قدم اول کاربران در این سیستم باید اقدامات امنتی را همواره در نظر گرفته و از پسورد های مناسب استفاده کنند و از استفاده اشتراکی اکانت خود با همکاران یا دوستان خود بپرهیزند و امکانات امنیتی را که از جانب مدیریت شبکه برای آنها فراهم شده است ،استفاده کنند،و در قدم بعدی مدیران باید جدیدترین مکانیسم ها و روش ها را برای امن سازی شبکه به کار ببرند و از تجهیزاتی استفاده کنند که حداکثر امنیت را به ارمغان آورد.

www.takbook.com

www.takbook.com

٤ فصل چهارم :چالش های امنیتی و راه کار ها در شبکه های وای فای

Chapter Four:Security Challenges and solution in Wi-Fi Networks

مراجع :**[10],[11]**

www.takbook.com

www.takbook.com

٤-١ مقدمه

موفقیت حیرت انگیز ۸۰۲.۱۱ به علت توسعه «اترنت بی سیم» است. همچنانکه ۸۰۲.۱۱ بـه ترقـی خـود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسـبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایـه ای از لینک رادیویی داشته باشند، تعدادی از ابزارهـا بـرای کمـک بـه آنهـا بـه خـدمت گرفتـه مـی شـوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شـبکه در اشـکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که بـه آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد.

در این فصل هفت مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LAN های بی سیم، راه حل آنها و در نهایت چگونگی ساخت یک شبکه بی سیم امن مورد بحث قرار می گیرد. بسیاری از پرسش ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می توانند استفاده کنند. یک آنالایزر از اولین خریـدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بـر عملکردهـای سـنتی تحلیـل پروتکـل و ابـزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سـیم را کنـد می کنند، استفاده شوند. این سلسله مقاله هریک از این «هفت مسأله امنیتی» را بررسی می کند و توضیح می دهد که چگونه و چرا آنالایزر بی سیم، یک ابزار حیاتی برای تضمین امنیت شبکه های بی سیم است.

٤-٢ مشکل اول: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنهـا، شـبکه هـا باید فریم های Beacon با پارامتر های شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن بـه یـک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فـریم هـای Beacon توسـط هـیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه ۸۰۲.۱۱ شما و پارامترهایش برای هر شخصی با یک کارت ۸۰۲.۱۱ قابل استفاده است. نفوذگران با آنتن های قوی می توانند شـبکه هـا را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجـام حملاتـی کننـد حتـی بـدون اینکـه بـه امکانات شما دسترسی فیزیکی داشته باشند.

www.takbook.com

www.takbook.com

شکل ٤.١ :نمونه ای از شبکه های بی سیم

٤-٢-١ راه حل مشکل اول: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه های بی سیم برای ایجاد امکان اتصال مناسب طراحی شده اند، اما می توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی سیم می تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی دهد. به هرحال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می تواند از خطر سوءاستفاده از شبکه بی سیم بکاهد.

تضمین امنیت روی یک شبکه بی سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال ها قرار دهند و مدیران شبکه باید به استفاده از VPNها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE 802.1x هستند. x۸۰۲.۱ انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالایزرهای باسیم سنتی می توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت ۸۰۲.۱۱ شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت 802.1x را دنبال می کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

www.takbook.com

www.takbook.com

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می دهند و می توانند چندین مسأله معمول امنیت 802.1x را تشخیص دهند. تعدادی از حملات روی شبکه های باسیم در سال های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه ها نشان می دهند. آنالایزرهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می کنند و به این ترتیب مدیران شبکه می توانند با به کارگیری سخت افزار و نرم افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی سیم بدون نظارت مهندسان امنیتی به کارگرفته شده باشند. موتورهای آنالیز خبره می توانند زمانی را که پیکربندی های پیش فرض کارخانه مورد استفاده قرار می گیرند، شناسایی کنند و به این ترتیب می توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالایزرها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

٤-٣ مسأله دوم: نقاط دسترسی نامطلوب

دسترسی آسان به شبکه های LAN بی سیم امری منفک از راه اندازی آسان آن نیست. این دو خصوصیت در هنگام ترکیب شدن با یکدیگر می توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی ! بخرد و بدون کسب اجازه ای خاص به کل شبکه متصل شود. بسیاری از نقاط دسترسی با اختیارات مدیران میانی عرضه می شوند و لذا دپارتمان ها ممکن است بتوانند LAN بی سیمشان را بدون صدور اجازه از یک سازمان IT مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح «نامطلوب» بکارگرفته شده توسط کاربران ، خطرات امنیتی بزرگی را مطرح می کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LAN های بی سیم آگاه نباشند. ثبت بسیاری از ورودها به شبکه نشان از آن دارد که ویژگی های امنیتی فعال نیستند و بخش بزرگی از آنها تغییراتی نسبت به پیکربندی پیش فرض نداشته اند و با همان پیکربندی راه اندازی شده اند.

www.takbook.com

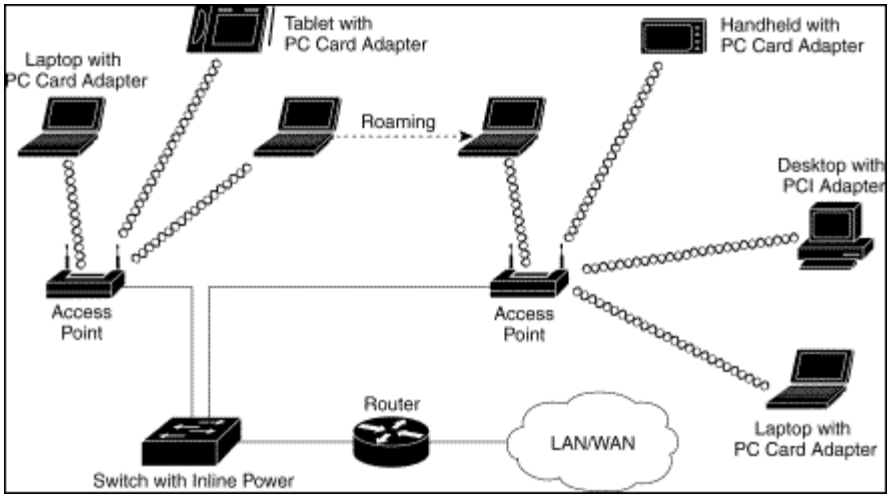
www.takbook.com

٤-۳-۱ راه حل مشکل دوم : رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه های امن نشده از اهمیت بالایی برخوردار است.

روش بدیهی یافتن این شبکه ها انجام همان کاری است که نفوذگران انجام می دهند: استفاده از یک آنتن و جستجوی آنها به این منظور که بتوانید قبل از نفوذگران این شبکه ها را پیدا کنید. نظارت های فیزیکی سایت باید به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت ها سریع تر انجام گیرد، امکان کشف استفاده های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفاده های غیرمجاز را بجز برای محیط های بسیار حساس، غیرقابل توجیه می کند. یک راهکار برای عدم امکان حضور دائم می تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می تواند استفاده تکنسین ها از اسکنرهای دستی در هنگام انجام امور پشتیبانی کاربران، برای کشف شبکه های غیرمجاز باشد.

یکی از بزرگترین تغییرات در بازار ۸۰۲.۱۱ در سال های اخیر ظهور a ۸۰۲.۱۱ به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های a ۸۰۲.۱۱ را بوجود آورد. خوشبختانه، a ۸۰۲.۱۱ از همان MAC پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجع به ۸۰۲.۱۱ و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استانداردa ۸۰۲.۱۱ و b ۸۰۲.۱۱را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست های دوباندی a/b ۸۰۲.۱۱ و کارت های ساخته شده با آنها به آنالایزرها اجازه می دهد که روی هر دو باند بدون تغییرات سخت افزاری کار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوب پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا g۸۰۲.۱۱ ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های a/b/g ۸۰۲.۱۱را مورد پذیرش قرار دهند.



www.takbook.com

www.takbook.com

بسیاری از ابزارها می توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می توانند در هر باند فرکانسی تعریف شده در ۸۰۲.۱۱ بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده فرکانسی را پویش کنند. حتی اگر شما استفاده از b ۸۰۲.۱۱ را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی a ۸۰۲.۱۱ را نیز پویش کند تا در طول یک بررسی کامل نیازی به جایگزین های سخت افزاری و نرم افزاری نباشد.

بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال های b ۸۰۲.۱۱ به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا ۱۱ از b ۸۰۲.۱۱ را می دهد. کانال های ۱۲ تا ۱٤ جزء مشخصات آن تعریف شده اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هرحال، بعضی کاربران ممکن است از نقطه دسترسی کانال های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال های مطابق با FCC از کانال های فرکانس بالاتر چشم پوشی کند. این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت دارد که بیرون باند فرکانسی مجاز بکارگرفته شده اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی های مجاز برحذر باشند. آنالایزرهای غیرفعال (Passive Analyzers) ابزار ارزشمندی هستند زیرا استفاده های غیرمجاز را تشخیص می دهند، اما چون توانی ارسال نمی کنند استفاده از آنها قانونی است.

مدیران شبکه همواره تحت فشار زمانی هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند. موتورهای جستجوی خبره به مدیران اجازه می دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده ای می شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

٤-٤ مشکل سوم استفاده غیرمجاز از سرویس

چندین شرکت مرتبط با شبکه های بی سیم نتایجی منتشر کرده اند که نشان می دهد اکثر نقاط دسترسی با تنها تغییرات مختصری نسبت به پیکربندی اولیه برای سرویس ارائه می گردند. تقریباً تمام نقاط دسترسی که با پیکربندی پیش فرض مشغول به ارائه سرویس هستند، WEP (Wired Equivalent Privacy) را فعال

www.takbook.com

www.takbook.com

نکرده اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنند گان محصولات استفاده می شـوند. بـدون WEP دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسـی بـاز مـی توانـد بـروز کنـد: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی کنند، و نیز ممکن است تنها توسط یک اسپم سـاز اتصال شما به ISPتان لغو شود.

٤-٤-١ راه حل مشکل سوم : طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجـاز بـه شـبکه اسـت. تأییـد هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صـدور اجـازه اسـت، زیـرا امتیـازات دسترسی برپایه هویت کاربر قرار دارند. روش های VPN که برای حفاظت از انتقال در لینـک رادیـویی بـه کارگرفته می شوند، تأیید هویت محکمی را ارائه می کنند. تخمین مخاطرات انجام شده توسط سـازمان هـا نشان می دهد که دسترسی به x۸۰۲.۱ باید توسط روش های تأیید هویت برپایه رمزنگاری تضمین شـود. از جمله این روش ها می توان به TLS (Transport Layer Security)، TTLS (Tunneled TLS) یا PEAP (Protected Extensible Authentication Protocol) اشاره کرد.

هنگامی که یک شبکه با موفقیت راه اندازی می شود، تضمین تبعیـت از سیاسـت هـای تاییـد هویـت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در ایـن راه حـل نیـز نظـارت های منظمی بر تجهیزات شبکه بی سیم باید انجام شود تا استفاده از مکانیسم های تأیید هویت و پیکربنـدی مناسب ابزارهای شبکه تضمین شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو باند فرکانسـیb ۸۰۲.۱۱ (باند GHz ISM 2.4) و ۸۰۲.۱۱a (GHz U-NII 5) تشخیص دهد و پارامترهای عملیـاتی مـرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسـیور دسـتی مـی تواند برای ردیابی موقعیت فیزیکی آن استفاده شود. آنالایزرها نیز می توانند برای تأیید پیکربندی بسیاری از پارامترهای نقاط دسترسی استفاده گردند و هنگامی که نقاط دسترسی آسیب پذیری های امنیتی را نمایان می کنند، علائم هشدار دهنده صوتی تولید کنند.

٤-٥ مشکل چهارم : محدودیت های سرویس و کارایی

LANهای بی سیم ظرفیت های ارسال محدودی دارند. شبکه هایb ۸۰۲.۱۱ سرعت انتقالی برابر با ۱۱ Mbps و شبکه های برپایه تکنولوژی جدیدa ۸۰۲.۱۱ نرخ انتقال اطلاعاتی تاMbps ٥٤ دارند. البته ماحصل مؤثر واقعی، به دلیل بالاسری لایه MAC، تقریباً تا نیمی از ظرفیت اسمی می رسد. نقاط دسترسی کنونی این ظرفیت محدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت مـی کننـد. تصـور اینکـه چگونـه برنامه های محلی احتمالاً چنین ظرفیت محدودی را اشغال می کنند یا چگونه یک نفوذگر ممکن است یـک حمله انکار سرویس (DoS) روی این منابع محدود طرح ریزی کند، سخت نیست.

www.takbook.com

www.takbook.com

ظرفیت رادیویی می تواند به چندین روش اشغال شود. ممکن است توسط ترافیکی که از سمت شبکه باسیم با نرخی بزرگتر از توانایی کانال رادیویی می آید، مواجه شود. اگر یک حمله کننده یک ping flood را از یک بخش اترنت سریع بفرستد، می تواند به راحتی ظرفیت یک نقطه دسترسی را اشغال کند. با استفاده از آدرس های broadcast امکان اشغال چندین نقطه دسترسی متصل به هم وجود دارد. حمله کننده همچنین می تواند ترافیک را به شبکه رادیویی بدون اتصال به یک نقطه دسترسی بی سیم تزریق کند. ۸۰۲.۱۱ طوری طراحی شده است که به چندین شبکه اجازه به اشتراک گذاری یک فضا و کانال رادیویی را می دهد. حمله کنندگانی که می خواهند شبکه بی سیم را از کار بیاندازند، می توانند ترافیک خود را روی یک کانال رادیویی ارسال کنند و شبکه مقصد ترافیک جدید را با استفاده از مکانیسم CSMA/CA تا آنجا که می تواند می پذیرد. مهاجمان بداندیش که فریم های ناسالم می فرستند نیز ظرفیت محدود را پر می کنند. همچنین ممکن است مهاجمان تکنیک های تولید پارازیت رادیویی را انتخاب کنند و اقدام به ارسال اطلاعات با نویز بالا به شبکه های بی سیم مقصد کنند.

بارهای بزرگ ترافیک الزاماً با نیات بدخواهانه تولید نمی شوند. انتقال فایل های بزرگ یا سیستم client/server ترکیبی ممکن است مقادیر بالایی از دیتا روی شبکه ارسال کنند. اگر تعداد کافی کاربر شروع به گرفتن اندازه های بزرگی از دیتا از طریق یک نقطه دسترسی کنند، شبکه شبیه سازی دسترسی dial-up را آغاز می کند.

٤-٥-١ راه حل مشکل چهارم : دیدبانی شبکه

نشان یابی مسائل کارایی با دیدبانی و کشف آنها آغاز می شود. مدیران شبکه بسیاری از کانال ها را برای کسب اطلاعات در مورد کارایی در اختیار دارند: از ابزارهای تکنیکی خاص مانند SNMP (Simple Network Management Protocol) گرفته تا ابزارهای بالقوه قوی غیرفنی مانند گزارش های کارایی کاربران. یکی از مسائل عمده بسیاری از ابزارهای تکنیکی، فقدان جزئیات مورد نیاز برای درک بسیاری از شکایت های کاربران در مورد کارایی است. آنالایزرهای شبکه های بی سیم می توانند با گزارش دهی روی کیفیت سیگنال و سلامت شبکه در مکان کنونی خود، کمک باارزشی برای مدیر شبکه باشند. مقادیر بالای ارسال های سرعت پایین می تواند بیانگر تداخل خارجی یا دور بودن یک ایستگاه از نقطه دسترسی باشد. توانایی نشان دادن سرعت های لحظه ای روی هر کانال، یک تصویر بصری قوی از ظرفیت باقی مانده روی کانال می دهد که به سادگی اشغال کامل یک کانال را نشان می دهد. ترافیک مفرط روی نقطه دسترسی می تواند با تقسیم ناحیه پوشش نقطه دسترسی به نواحی پوشش کوچک تر یا با اعمال روش شکل دهی ترافیک در تلاقی شبکه بی سیم با شبکه اصلی تعیین شود.

www.takbook.com

www.takbook.com

در حالیکه هیچ راه حل فنی برای آسیب پذیری های ناشی از فقدان تأیید هویت فریم های کنترل و مدیریت وجود ندارد، مدیران می توانند برای مواجهه با آنها گام هایی بردارند. آنالایزرها اغلب نزدیک محل های دردسرساز استفاده می شوند تا به تشخیص عیب کمک کنند و به صورت ایده آل برای مشاهده بسیاری از حملات DoS کار گذاشته می شوند. مهاجمان می توانند با تغییر دادن فریم های ۸۰۲.۱۱ با استفاده از یکی از چندین روش معمول واسط های برنامه نویسی ۸۰۲.۱۱ موجود، از شبکه سوءاستفاده کنند. حتی یک محقق امنیتی ابزاری نوشته است که پیام های قطع اتصال فرستاده شده توسط نقاط دسترسی به کلاینت ها را جعل می کند. بدون تأیید هویت پیام های قطع اتصال بر اساس رمزنگاری، کلاینت ها به این پیام های جعلی عمل می کنند و اتصال خود را از شبکه قطع می کنند. تا زمانی که تأیید هویت به صورت یک فریم رمزشده استاندارد درنیاید، تنها مقابله علیه حملات جعل پیام، مکان یابی حمله کننده و اعمال عکس العمل مناسب است.

٤-٦ مشکل پنجم جعل MAC و session ربایی!

شبکه های ۸۰۲.۱۱ فریم ها را تأیید هویت نمی کنند. هر فریم یک آدرس مبداء دارد، اما تضمینی وجود ندارد که ایستگاه فرستنده واقعاً فریم را ارسال کرده باشد! در واقع همانند شبکه های اترنت سنتی، مراقبتی در مقابل جعل مبداء آدرس ها وجود ندارد. نفوذگران می توانند از فریم های ساختگی برای هدایت ترافیک و تخریب جداول(Address Resolution Protocol) ARP استفاده کنند. در سطحی بسیار ساده تر، نفوذگران می توانند آدرس های (Medium Access Control) MAC ایستگاه های در حال استفاده را مشاهده کنند و از آن آدرس ها برای ارسال فریم های بدخواهانه استفاده کنند. برای جلوگیری از این دسته از حملات، مکانیسم تصدیق هویت کاربر برای شبکه های ۸۰۲.۱۱ در حال ایجاد است. با درخواست هویت از کاربران، کاربران غیرمجاز از دسترسی به شبکه محروم می شوند. اساس تصدیق هویت کاربران استاندارد x ۸۰۲.۱است که در ژوئن ۲۰۰۱ تصویب شده است. x ۸۰۲.۱می تواند برای درخواست هویت از کاربران به منظور تأیید آنان قبل از دسترسی به شبکه مورد استفاده قرار گیرد، اما ویژگی های دیگری برای ارائه تمام امکانات مدیریتی توسط شبکه های بی سیم مورد نیاز است.

نفوذگران می توانند از فریم های جعل شده در حملات اکتیو نیز استفاده کنند. نفوذگران علاوه بر ربودن نشست ها (sessions) می توانند از فقدان تصدیق هویت نقاط دسترسی بهره برداری کنند. نقاط دسترسی توسط پخش فریم های Beacon (چراغ دریایی) مشخص می شوند. فریم های Beacon توسط نقاط دسترسی ارسال می شوند تا کلاینت ها قادر به تشخیص وجود شبکه بی سیم و بعضی موارد دیگر شوند. هر ایستگاهی که ادعا می کند که یک نقطه دسترسی است و(Service Set Identifier) SSID که معمولاً network name نیز نامیده می شود، منتشر می کند، به عنوان بخشی از شبکه مجاز به نظر خواهد رسید. به

www.takbook.com

www.takbook.com

هرحال، نفوذگران می توانند به راحتی تظاهر کنند که نقطه دسترسی هستند، زیرا هیچ چیز در ۸۰۲.۱۱ از نقطه دسترسی نمی خواهد که ثابت کند واقعاً یک نقطه دسترسی است. در این نقطه، یک نفوذگر می تواند با طرح ریزی یک حمله man-in-the-middle گواهی های لازم را سرقت کند و از آنها برای دسترسی به شبکه استفاده کند. خوشبختانه، امکان استفاده از پروتکل هایی که تأیید هویت دوطرفه را پشتیبانی می کنند در x۸۰۲.۱ وجود دارد. با استفاده از پروتکل TLS (Transport Layer Security)، قبل از اینکه کلاینت ها گواهی های هویت خود را ارائه کنند، نقاط دسترسی باید هویت خود را اثبات کنند. این گواهی ها توسط رمزنگاری قوی برای ارسال بی سیم محافظت می شوند. ربودن نشست حل نخواهد شد تا زمانی که MAC ۸۰۲.۱۱ تصدیق هویت در هر فریم را به عنوان بخشی از I ۸۰۲.۱۱ بپذیرد.

٤-٦-١ راه حل شماره۵ : پذیرش پروتکل های قوی و استفاده از آنها

تا زمان تصویب i ۸۰۲.۱۱ جعل MAC یک تهدید خواهد بود. مهندسان شبکه باید روی خسارت های ناشی از جعل MAC تمرکز کنند و شبکه های بی سیم را تا آنجا که ممکن است از شبکه مرکزی آسیب پذیرتر جدا کنند. بعضی راه حل ها جعل AP (نقاط دسترسی) را کشف می کنند و به طور پیش فرض برای مدیران شبکه علائم هشدار دهنده تولید می کنند تا بررسی های بیشتری انجام دهند. در عین حال، می توان فقط با استفاده از پروتکل های رمزنگاری قوی مانند IPSec از نشست ربایی! جلوگیری کرد. آنالایزرها می توانند در بخشی از تحلیل فریم های گرفته شده، سطح امنیتی مورد استفاده را تعیین کنند. این تحلیل می تواند در یک نگاه به مدیران شبکه بگوید آیا پروتکل های امنیتی مطلوبی استفاده می شوند یا خیر.

علاوه بر استفاده از پروتکل های VPN قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی کاربر با استفاده از x ۸۰۲.۱ داشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق x ۸۰۲.۱، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت x ۸۰۲.۱ ارائه می کند. هنگام انجام نظارت بر سایت، آنالایزر نوع تصدیق هویت را مشخص می کند و این بررسی به مدیران شبکه اجازه می دهد که محافظت از کلمات عبور توسط رمزنگاری قوی را تضمین کنند.

٤-٧ مشکل ششم: تحلیل ترافیک و استراق سمع

۸۰۲.۱۱ هیچ محافظتی علیه حملاتی که بصورت غیرفعال (passive) ترافیک را مشاهده می کنند، ارائه نمی کند. خطر اصلی این است که ۸۰۲.۱۱ روشی برای تامین امنیت دیتای در حال انتقال و جلوگیری از استراق سمع فراهم نمی کند. Header فریم ها همیشه «in the clear» هستند و برای هرکس با در اختیار داشتن یک آنالایزر شبکه بی سیم قابل مشاهده هستند. فرض بر این بوده است که جلوگیری از استراق سمع در مشخصات WEP (Wired Equivalent Privacy) ارائه گردد. بخش زیادی در مورد رخنه های WEP نوشته شده است که فقط از اتصال ابتدایی بین شبکه و فریم های دیتای کاربر محافظت می کند. فریم

www.takbook.com

www.takbook.com

های مدیریت و کنترل توسط WEP رمزنگاری و تصدیق هویت نمی شوند و به این ترتیب آزادی عمل زیادی به یک نفوذگر می دهد تا با ارسال فریم های جعلی اختلال به وجود آورد. پیاده سازی های اولیه WEP نسبت به ابزارهای crack مانند AirSnort و WEPcrack آسیب پذیر هستند، اما آخرین نسخه ها تمام حملات شناخته شده را حذف می کنند. به عنوان یک اقدام احتیاطی فوق العاده، آخرین محصولات WEP یک گام فراتر می روند و از پروتکل های مدیریت کلید برای تعویض کلید WEP در هر پانزده دقیقه استفاده می کنند. حتی مشغول ترین LAN بی سیم آنقدر دیتا تولید نمی کند که بتوان در پانزده دقیقه کلید را بازیافت کرد.

٤-۷-۱ راه مشکل ششم : انجام تحلیل خطر

هنگام بحث در مورد خطر استراق سمع، تصمیم کلیدی برقراری توازن بین خطر استفاده از WEP تنها و پیچیدگی بکارگیری راه حل اثبات شده دیگری است. در وضعیت فعلی برای امنیت لایه لینک، استفاده از WEP با کلیدهای طولانی و تولیدکلید پویا توصیه می شود. WEP تا حد زیادی مورد کنکاش قرار گرفته است و پروتکل های امنیتی علیه تمام حملات شناخته شده تقویت شده اند. یک قسمت بسیار مهم در این تقویت، زمان کم تولید مجدد کلید است که باعث می شود نفوذگر نتواند در مورد خصوصیات کلید WEP ، قبل از جایگزین شدن، اطلاعات عمده ای کسب کند.

اگر شما استفاده از WEP را انتخاب کنید، باید شبکه بی سیم خود را نظارت کنید تا مطمئن شوید که مستعد حمله AirSnort نیست. یک موتور آنالیز قوی به طور خودکار تمام ترافیک دریافت شده را تحلیل می کند و ضعف های شناخته شده را در فریم های محافظت شده توسط WEP بررسی می کند. همچنین ممکن است بتواند نقاط دسترسی و ایستگاه هایی را که WEP آنها فعال نیست نشان گذاری کند تا بعداً توسط مدیران شبکه بررسی شوند. زمان کوتاه تولید مجدد کلید ابزار بسیار مهمی است که در کاهش خطرات مربوط به شبکه های بی سیم استفاده می شود. بعنوان بخشی از نظارت سایت، مدیران شبکه می توانند از آنالایزرهای قوی استفاده کنند تا مطمئن شوند که سیاست های تولید کلید مجدد WEP توسط تجهیزات مربوطه پیاده سازی شده اند

اگر از LAN بی سیم شما برای انتقال دیتای حساس استفاده می شود، ممکن است WEP برای نیاز شما کافی نباشد. روش های رمزنگاری قوی مانند SSH، SSL و IPSec برای انتقال دیتا به صورت امن روی کانال های عمومی طراحی شده اند و برای سال ها مقاومت آنها در برابر حملات ثابت شده است، و یقیناً سطوح بالاتری از امنیت را ارائه می کنند. نمایشگرهای وضعیت نقاط دسترسی می توانند بین نقاط دسترسی که از WEP، 802.1x و VPN استفاده می کنند، تمایز قائل شوند تا مدیران شبکه بتوانند بررسی کنند که آیا در آنها از سیاست های رمزنگاری قوی تبعیت می شود یا خیر.

www.takbook.com

www.takbook.com

علاوه بر استفاده از پروتکل های VPN قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی کاربر با استفاده از x ۸۰۲.۱ داشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق x۸۰۲.۱، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت x ۸۰۲.۱ ارائه می کند. آنالایزر هنگام انجام نظارت بر سایت، نوع تصدیق هویت را مشخص می کند و این بررسی به مدیران شبکه اجازه می دهد که محافظت از کلمات عبور توسط رمزنگاری قوی را تضمین کنند.

٤-٨ مشکل هفتم: حملات سطح بالاتر

هنگامی که یک نفوذگر به یک شبکه دسترسی پیدا می کند، می تواند از آنجا به عنوان نقطه ای برای انجام حملات به سایر سیستم ها استفاده کند. بسیاری از شبکه ها یک پوسته بیرونی سخت دارند که از ابزار امنیت پیرامونی تشکیل شده، به دقت پیکربندی شده و مرتب دیده بانی می شوند. اگرچه درون پوسته یک مرکز آسیب پذیر نرم قرار دارد. LANهای بی سیم می توانند به سرعت با اتصال به شبکه های اصلی آسیب پذیر مورد استفاده قرار گیرند، اما به این ترتیب شبکه در معرض حمله قرار می گیرد. بسته به امنیت پیرامون، ممکن است سایر شبکه ها را نیز در معرض حمله قرار دهد، و می توان شرط بست که اگر از شبکه شما به عنوان نقطه ای برای حمله به سایر شبکه ها استفاده شود، حسن شهرت خود را از دست خواهید داد.

٤-٨-١ راه حل مشکل هفتم : هسته را از LAN بی سیم محافظت کنید

به دلیل استعداد شبکه های بی سیم برای حمله، باید به عنوان شبکه های غیرقابل اعتماد مورد استفاده قرار بگیرند. بسیاری از شرکت ها درگاه های دسترسی guest در اتاق های آموزش یا سالن ها ارائه می کنند. شبکه های بی سیم به دلیل احتمال دسترسی توسط کاربران غیرقابل اعتماد می توانند به عنوان درگا ه های دسترسی guest تصور شوند. شبکه بی سیم را بیرون منطقه پیرامون امنیتی شرکت قرار دهید و از تکنولوژی کنترل دسترسی قوی و ثابت شده مانند یک فایروال بین LAN بی سیم و شبکه مرکزی استفاده کنید، و سپس دسترسی به شبکه مرکزی را از طریق روش های VPN تثبیت شده ارائه کنید.

٤-٩ چند نکته در مورد امن سازی شبکه های وای فای

٤-٩-١ کلمه عبور پیش فرض مدیر سیستم(administrator) را روی نقاط دسترسی و مسیریاب های بی‌سیم تغییر دهید.

اغلب نقاط دسترسی (Access Point)و مسیریاب‌های بی‌سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می‌کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می‌کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم

www.takbook.com

www.takbook.com

می‌کنند . نام کاربری معمول admin یا administrator و کلمه عبور یا خالی است یا کلماتی مثل admin ، public، password و .... می‌باشد.

اولین گام برای افزایش امنیت شبکه بی‌سیم تغییر کلمه عبور پیش‌فرض نقاط دسترسی و مسیریاب‌های بی‌سیم بلافاصله پس از نصب است. اغلب ابزارها اجازه تغییر نام کاربری را نمی‌دهند اما اگر ابزارهای شما این امکان را می‌دهند، اکیدا توصیه می‌شود که نام کاربری را هم تغییر دهید.

برای امن نگه‌داشتن شبکه در آینده، می‌بایست به‌طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از ۳۰ تا ۹۰ روز تغییر دهید.

٤-۹-۲ فعال‌سازی قابلیت WPA/WEP

WPA (WiFi Protected Access) یک استاندارد امنیتی برای شبکه‌های بی‌سیم است (با Windows XP Product Activation اشتباه نشود). برای استفاده از WPA با Windows XP باید Clientهای دارای Windows XP را به صورت دستی patch کنید و هم‌چنین مطمئن شوید کارت شبکه‌ها و نقاط دسترسی به درستی پیکربندی شده‌اند.برای پیکربندی WPA در شبکه با clientهای دارای ویندوز XP مراحل زیر را انجام دهید:

۱. نوشتار Overview of the WPA wireless security update in Windows XP را مطالعه کنید.
۲. بررسی کنید که تمام Client ها حداقل Service Pack1 داشته باشند.
۳. روی هر Client بررسی کنید که کارت شبکه با سرویس WZC(Windows Zero Configuration) سازگار باشد.
٤. برای هر client وصله Windows XP Support Patch for Wi-Fi Protected Access را بارگزاری و نصب کنید.
۵. تغییرات لازم برای نقاط دسترسی بی‌سیم از گام ۱ را اعمال کنید.

٤-۹-۳ تغییر SSID پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه SSID(Service Set Identifier) هستند که توسط تولیدکنندگان به‌طور پیش‌فرض انتخاب می‌شود. SSID از ابزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب SSIDهای پیش فرض کلمات ساده ای مثل wireless، netgear، linksys، default و ... هستند. هرچند نفوذگر صرفا با دانستن SSID قادر به نفوذ به شبکه شما نیست ولی این مساله به عنوان یک نقطه شروع خوب برای نفوذگر به حساب می آید. زمانی که کسی شبکه ای با

www.takbook.com

www.takbook.com

SSID پیش فرض بیابد، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است، ترغیب به نفوذ به شبکه می‌شود.

SSID می تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام clientها نیز اعمال شود. برای افزایش امنیت شبکه های بی سیم، نام پیش فرض SSID را تغییر دهید. در انتخاب SSID توصیه های زیر را در نظر داشته باشید:

۱. از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از SSID استفاده نکنید.

۲. از کلمات عبور نام کاربری ویندوزتان یا emailتان یا ... استفاد نکنید.

۳. با استفاده از عباراتی مثل ""TOP_SECRET، "FUNNY_BOX"" و ... نفوذگران را وسوسه نکنید.!!!

٤. از ترکیب حروف و اعداد استفاده کنید.

٥. عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید.

٦. هرچند ماه یک بار SSIDتان را تغییر دهید.

٤-۹-٤ قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب‌های بی‌سیم فعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم دارای قابلیتی به نام پالایش آدرس MAC (MAC Address Filtering) هستند. این مشخصه اغلب به‌طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی سیم تان این قابلیت را فعال کنید. در صورتی که این قابلیت فعال نباشد، هر clientای با دانستن SSID شبکه شما (در نظر داشته باشید که فهمیدن SSID کار بسیار ساده ای است) شاید چند پارامتر امنیتی دیگر مثل کلید رمزگذاری (در صورتی که قابلیت WEP فعال باشد) می تواند به شبکه شما وصل شود.

برای تنظیم قابلیت پالایش آدرس MAC شما به عنوان مدیر شبکه بی سیم باید لیست clientهایی که مجازند به شبکه وصل شوند را پیکربندی کنید. ابتدا آدرس MAC هر client را از طریق سیستم عامل یا ابزارهای پیکربندی به دست آورید و سپس آن ها را در صفحه پیکربندی نقاط دسترسی و مسیریاب های بی سیم وارد کنید و نهایتا قابلیت پالایش را فعال کنید. از این پس هر درخواست اتصال به شبکه بی سیم که برسد آدرس MAC آن با لیست تنظیم شده بررسی شده و در صورتی که در لیست نباشد اجازه اتصال به

www.takbook.com

www.takbook.com

شبکه را نمی یابد. البته باید نوجه داشت که نفوذگران با جعل آدرس MAC (MAC Spoofing) قادرند به شبکه بی سیم شما وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

٤-۹-۵ قابلیت همه‌پخشی SSID را روی نقاط دسترسی و مسیریاب‌های بی‌سیم غیرفعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم به طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می کنند. این مشخصه برای این است که clientها بتواندد به‌طور پویا شبکه های بی سیم را تشخیص دهند و بین آن ها جابه جا شوند (از شبکه ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برای hotspotهای تجاری و سیار طراحی شده است که clientهای زیادی می آیند و می روند ولی برای شبکه های خانگی لازم نیست. از آن جایی که SSID به صورت واضح پخش می شود و هیچ رمزگذاری روی آن صورت نمی گیرد، به دست آوردن آن توسط نفوذگران کار راحتی است. همان‌طور که در گام ۳ اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک تر می شود.

در یک شبکه بی سیم بحث roaming (جابه جایی بین دو شبکه بی سیم) مطرح نیست و پخش کردن SSID هیچ ضرورتی ندارد. برای افزایش امنیت شبکه بی سیم باید این قابلیت را غیرفعال کنید. یک بار که client شما با SSID درست پیکربندی شد دیگر نیازی به پیغام های همه‌پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه‌پخشی SSID فقط یکی از تکنیک‌های محکم‌سازی و افزایش امنیت شبکه‌های بی سیم است. این روش ۱۰۰ درصد موثر نیست و نفوذگرها هنوز می توانند با sniff کردن پیغام های مختلف پخش شده در پروتکل WiFi، SSID را تشخیص دهند. در واقع تکنیک هایی مثل غیرفعال کردن همه پخشی SSID باعث می شئد که شبکه بی سیم شما هدف راحتی برای نفوذگران نباشد.

٤-۹-٦ به شبکه های WiFi باز وصل نشوید

مطمئن شوید که تنظیمات سیستم به گونه ای است که مانع اتصال خودکار به نقاط دسترسی ناامن شود.اتصال به یک شبکه WiFi باز مثل یک hotspot یا مسیریاب بی‌سیم آزاد، کامپیوتر شما را در معرض خطرات فراوانی قرار می دهد. هرچند به طور معمول این امکان فعال نیست ولی اغلب کامپیوترها دارای تنظیماتی هستند که امکان اتصال خودکار بدون اطلاع کاربر را فراهم می‌کنند. این تنظیمات به‌جز در موارد ضروری و به‌طور موقت نباید فعال باشد.

برای بررسی این‌که آیا اتصال خودکار به شبکه‌های WiFi باز، مجاز است یا نه، تنظیمات بی‌سیم کامپیوتر را بررسی کنید. برای مثال در کامپیوترهایی که دارای Windows XP هستند، تنظیمات بی‌سیم

www.takbook.com

www.takbook.com

Automatically connect to non-preferred networks نامیده می‌شود. برای بررسی مراحل زیر را انجام دهید:

۱. از منوی start به گزینه Windows Control Panel بروید.

۲. به گزینه Network Connections بروید

۳. بر روی Wireless Network Connection کلیک راست کنید و گزینه Properties را انتخاب کنید.

٤. روی گزینه Wireless Networks کلیک کنید.

۵.بر روی دکمه Advanced کلیک کنید.

٦. گزینه Automatically connect to non-preferred networks را پیدا کنید، اگر انتخاب شده بود این تنظیمات فعال است در غیر این صورت غیرفعال است.

اگرچه در Windows XP به‌طور پیش فرض Automatically connect to non-preferred networks فعال نیست، برخی کاربران برای سهولت اتصال به شبکه خودشان آن را فعال می‌کنند. کاربران باید شبکه خودشان را به عنوان Windows XP Preferred networks تنظیم کنند که اجازه اتصال خودکار را می‌دهد و اتصال خودکار به بقیه شبکه‌ها را غیرفعال کنند.

٤-۹-۷ به تجهیزات آدرس (IP) ایستا اختصاص دهید.

اختصاص آدرس ایستا جایگزینی برای پروتکل DHCP است. اختصاص آدرس پویا با استفاده از DHCP راحت تر است و هم چنین به کامپیوترهای سیار اجازه می دهد که بین شبکه های مختلف جابه جا شوند.

آدرس دهی ایستا نیز مزایایی دارد، از جمله:

- آدرس ثابت ترجمه آدرس را بهتر پشتیبانی می کند، بنابراین یک کامپیوتر روی شبکه با نام دامنه اش به طور مطمئن قابل دستیابی است. مخصوصا سرورهایی مثل سرور وب و سرور FTP بهتر است آدرس ایستا داشته باشند.
- استفاده از آدرس دهی ایستا در مقابل DHCP محافظت بیشتری در برابر حملات امنیتی فراهم می کند.
- برخی تجهیزات شبکه پروتکل DHCP را پشتیبانی نمی کنند.
- استفاده از آدرس دهی ایستا برای تمام اجزای شبکه تضمین می کند که ناسازگاری آدرس ها رخ نمی دهد.

www.takbook.com

www.takbook.com

آدرس های ایستا باید از محدوده آدرس های خصوصی استاندارد انتخاب شود از جمله:

۱."۱۰.۰.۰.۰" تا "۱۰.۲۵۵.۲۵۵.۲۵۵"

۲."۱۷۲.۱۶.۰.۰" تا "۱۷۲.۳۱.۲۵۵.۲۵۵"

۳. "۱۹۲.۱۶۸.۰.۰" تا "۱۹۲.۱۶۸.۲۵۵.۲۵۵"

این محدوده ها تعداد زیادی آدرس را پشتیبانی می کنند. برخلاف تصور اکثر افراد، تمام آدرس های این محدوده ها نمی توانند انتخاب شوند. برای انتخاب آدرس درست نکات زیر را مدنظر داشته باشد:

۱. آدرس هایی که با "۰" یا "۲۵۵" تمام می شوند را انتخاب نکنید. این آدرس ها برا ی استفاده پروتکل های شبکه رزرو شده اند.

۲. آدرس های ابتدای یک محدود آدرس خصوصی را انتخاب نکنید. آدرس هایی مثل "۱۰.۰.۰.۱" یا "۱۹۲.۱۶۸.۰.۱" معمولا به مسیریاب ها ی شبکه اختصاص می یابند. این آدرس ها اولین آدرس هایی هستند که معمولا یک نفوذگر تلاش می کند به آن ها نفوذ کند، بنابراین بهتر است از آن ها استفاده نکنید.

۳. از آدرس هایی که خارج از محدوده mask شبکه شما می باشد استفاده نکنید. برای مثال، برای پشتیبانی تمام آدرس های محدوده "۱۰.x.x.x"، mask شبکه برای تمام سیستم ها باید به "۲۵۵.۰.۰.۰" تنظیم شود، در غیراین صورت برخی آدرس های ایستای این محدوده کار نمی کنند.

٤-۹-۸ قابلیت فایروال را روی تمام کامپیوترها و مسیریاب‌ها فعال کنید

یکی از آسان ترین و ارزان ترین راه ها برای محافظت از شبکه در برابر حملات استفاده از فایروال شخصی است.

٤-۹-۹ مسیریاب‌ها و نقاط دسترسی را در مکان‌های امن قرار دهید

کارآیی شبکه Wi-Fi به میزان زیادی بستگی به قدرت سیگنال مسیریاب یا نقطه دسترسی بی سیم دارد. اگر یک client بی سیم خارج از محدوده قدرت سیگنال قرار بگیرد ارتباط آن با شبکه قطع می شود یا ارتباط بسیار ضعیف می‌باشد. Clientهای بی سیم واقع شده در لبه شبکه ممکن است به دفعات زیاد ارتباطشان قطع شود، ولی حتی زمانی که یک Client بی سیم در محدوده قدرت سیگنال هم باشد، کارآیی شبکه از مواردی همچون فاصله، انسداد، یا تداخل تاثیر می گیرد.

برای تعیین محل قرار گرفتن تجهیزات بی سیم نکات زیر را مدنظر داشته باشد:

www.takbook.com

www.takbook.com

- اولین و مهم ترین نکته این است که، از قبل جایی را برای مسیریاب یا نقطه دسترسی بی سیم در نظر نگیرید. سعی کنید تجهیزات را در چندین نقطه متفاوت امتحان کنید. با وجود این که روش آزمون و خطا راهکار علمی برای یافتن محل قرارگیری تجهیزات بی سیم نیست اما از دیدگاه عملی بهترین روش برای به دست آوردن حداکثر کارآیی است.
- سعی کنید مسیریاب یا نقطه دسترسی بی سیم را نزدیک به مرکز قرار دهید. Clientهایی که از ایستگاه مرکزی فاصله بیشتری دارند، در مقایسه با Clientهایی که نزدیک ایستگاه مرکزی هستند ، فقط از ۱۰ تا ۵۰ درصد پهنای باند بهره مند می شوند.
- تا حدامکان سعی کنید از موانع فیزیکی دوری کنید. هرگونه مانعی در فاصله خط دید بین Client و ایستگاه مرکزی باعث کاهش قدرت سیگنال می شود. دیوارهای آجری، خشتی، یا ساروج اندود بیش ترین تاثیر منفی را دارند ولی موانع دیگر نیز باعث کاهش قدرت سیگنال می شوند.
- تا حد امکان از سطوح بازتابی اجتناب کنید. برخی سطوح بازتابی مثل پنجره ها، آینه ها و ... باعث کاهش محدوده قدرت سیگنال های WiFi و در نتیجه کارآیی شبکه می شود.
- مسیریاب یا نقطه دسترسی بی سیم را حداقل به فاصله یک متر از دیگر تجهیزاتی که در محدوده فرکانس مشابه سیگنال بی سیم می فرستند قرار دهید. این ابزارها می تواند شامل تلفن بی سیم، اجاق های مایکروویو و ... باشد.
- همچنین مسیریاب یا نقطه دسترسی بی سیم را دور از تجهیزات الکتریکی که باعث ایجاد تداخل می شوند قرار دهید.
- اگر مکان مناسبی که پیدا کردید فقط به طور مرزی قابل قبول شود، آنتن های ایستگاه مرکزی را برای بهبود کارآیی تنظیم کنید. می توانید آنتن های مسیریاب و نقاط دسترسی بی سیم را بچرخانید و محل آن را تغییر دهید، دستورالعمل های کارخانه سازنده را اعمال کنید تا بهترین کارآیی را به دست آورید.
- اگر با استفاده از این نکات و دستورالعمل ها باز هم مشکل دارید، می توانید به عنوان مثال آنتن های خود را تغییر دهید، یک تکرارکننده نصب کنید، یا در مواردی ایستگاه مرکزی دیگری پیکربندی و استفاده کنید.

٤-۹-۱۰ در فواصل زمانی طولانی که از شبکه استفاده نمی‌کنید تجهیزات را خاموش کنید.

اغلب ارتباطات اینترنت باندپهن همیشه برخط هستند. به همین خاطر دارندگان شبکه ترجیح می دهند اکثر تجهیزات شبکه مثل مسیریاب یا مودم روشن بماند حتی اگر برای مدت های طولانی بدون استفاده

www.takbook.com

www.takbook.com

باشند.ولی آیا شبکه های محلی هم لازم است همیشه روشن بمانند؟ خاموش کردن تجهیزات شبکه چه مزایا و معایبی دارد؟

در ادامه برخی از مزایا و معایب خاموش کردن تجهیزات شبکه را هنگامی که استفاده ای از آن ها نمی شود، بررسی می کنیم:

امنیت: خاموش کردن تجهیزات شبکه زمانی که در حال استفاده نیستند، باعث افزایش امنیت شبکه می شود. زمانی که تجهیزات شبکه خاموش باشند نفوذگران قادر به انجام کاری نیستند.

صرفه جویی در مصرف برق: خاموش کردن تجهیزات شبکه باعث صرفه جویی در هزینه ها می شود. در برخی کشورها این صرفه جویی چندان قابل توجه نیست اما در برخی کشورها نیز به علت بالا بودن هزینه انرژی میزان قابل توجهی است.

محافظت در برابر اعوجاج سیگنال: جدا کردن تجهیزات شبکه باعث جلوگیری از خرابی های احتمالی منتج از اعوجاج سیگنال می شود. ممکن است گفته شود که محافظ ها هم قادرند از ابزارها در برابر اعوجاج مراقبت کنند ولی این محافظ ها به خصوص انواع ارزان قیمت آن قادر به مراقبت در برابر نوسانات شدید نیستند.

قابلیت اطمینان سخت افزار: قطع و وصل مدام منبع انرژی تجهیزات شبکه باعث کاهش طول عمر آن ها می شود. دیسک درایوها اغلب آسیب پذیر هستند. به عبارت دیگر، دمای زیاد هم باعث کاهش طول همه ابزارهای شبکه می شود. همیشه روشن گذاشتن تجهیزات شبکه در مقایسه با زمانی که تجهیزات گهگاه خاموش می شوند، احتمالا باعث آسیب های بیش تری می شود.

قابلیت اطمینان ارتباطات: بعد از خاموش و روشن کردن تجهیزات ممکن است فرآیند برقراری ارتباط مجدد با خطا مواجه شود. باید فرآیند راه اندازی مجدد را با احتیاط دنبال کنید. به عنوان مثال باید ابتدا مودم های باندپهن روشن شوند و ابزارهای دیگر پس از این که مودم آماده شد، روشن شوند. همچنین اگر هنگام راه اندازی یا نصب با خطایی مواجه می شوید حتما راه حلی برای آن پیدا کنید در غیراین صورت ممکن است در آینده منجر به مشکلات بزرگ تری شود.

سهولت: تجهیزات شبکه مثل مسیریاب بی سیم یا مودم ممکن است در مکان هایی مثل سقف یا مکان هایی که دسترسی به آن ها سخت است قرار داشته باشد. هنگام خاموش کردن این تجهیزات احتیاط نموده و به جای استفاده از دکمه خاموش و روشن کردن تجهیزات، رویه های توصیه شده توسط کارخانه سازنده را حتما رعایت کنید.

www.takbook.com

www.takbook.com

٤-۱۰ پنج اشتباه متداول درباره امنیت شبکه‌های بی‌سیم

٤-۱۰-۱ دیواره آتش= تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

اغلب سازمان‌ها، شبکه‌های بی‌سیم را به‌عنوان بخش مکملی برای شبکه سیمی خود راه‌اندازی می‌کنند. اتصال بی‌سیم، یک رسانه فیزیکی است و برای تأمین امنیت آن نمی‌توان تنها به وجود یک دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه‌های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آن‌ها، نوعی تهدید علیه شبکه به‌شمار می‌روند. علاوه بر این نقاط دسترسی، باید نگران لپ‌تاپ‌های بی‌سیم متصل به شبکه سیمی خود نیز باشید. یافتن لپ‌تاپ‌های متصل به شبکه سیمی که یک کارت شبکه بی‌سیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب می‌شود. در اغلب موارد این لپ‌تاپ‌ها توسط SSID شبکه‌هایی را که قبلاً مورد دسترسی قرار داده‌اند، جست‌وجو می‌کنند و در صورت یافتن آن‌ها صرف‌نظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بی‌سیم در همسایگی شبکه فعلی قرار داشته باشد، به‌طور خودکار به آن وصل می‌شوند. به محض این‌که لپ‌تاپ به یک شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله‌ها به کار گیرند. در این شرایط علاوه بر افشای اطلاعات مهم لپ‌تاپ، مهاجم می‌تواند از آن به عنوان نقطه شروعی برای حمله به شبکه سیمی استفاده کند. مهاجم درصورت انجام چنین اقداماتی، به‌طور کامل از دیواره آتش شبکه عبور می‌کند.

اغلب سازمان‌ها دیواره آتش شبکه را به‌گونه‌ای تنظیم می‌کنند که از آن‌ها در برابر حمله‌های مبتنی بر اینترنت محافظت می‌کند، اما امنیت شبکه در مقابل خروج از شبکه (Extrusion) و خروج غیرمجاز اطلاعات (leakage) تأمین نمی‌شود. اصولاً زمانی که درباره خروج غیرمجاز اطلاعات صحبت می‌کنیم، منظورمان خروج اطلاعات از شبکه است.

بسیاری از سازمان‌ها تنظیمات دیواره آتش را برای کنترل ترافیک اطلاعات خروجی به‌درستی انجام نمی‌دهند. در نتیجه این سهل‌انگاری معمولاً اطلاعات محرمانه سازمان به خارج منتقل می‌شود. به‌عنوان مثال، یکی از متداول‌ترین مواردی که هنگام انجام آزمون‌های امنیتی با آن مواجه شدیم، خروج اطلاعات شبکه سیمی از طریق نقاط دسترسی بی‌سیم بود. در این آزمون‌ها با استفاده از یک نرم‌افزار ردیاب (Sniffer) بی‌سیم توانستیم حجم زیادی از ترافیک اطلاعات خروجی ناخواسته را شناسایی کنیم. این اطلاعات شامل داده‌های مربوط به STP (سرنام Speaning Tree Protocol،IGRP) سایر سرویس‌های شبکه و حتی در مواردی اطلاعات مربوط به NetBIOS بودند.

چنین نقطه ضعفی شبکه را به یک اسباب سرگرمی برای مهاجم تبدیل می‌کند. در حقیقت، نفوذ به چنین شبکه‌ای حتی نیازمند یک اسکن فعال یا حمله واقعی نیست. به واسطه ردیابی جریان اطلاعاتی یک شبکه

www.takbook.com

www.takbook.com

بی‌سیم علاوه بر شناسایی توپولوژی بخش سیمی آن می‌توان اطلاعات مربوط به تجهیزات حیاتی شبکه و حتی گاهی اطلاعات مربوط به حساب‌های کاربری را به‌دست آورد.

٤-١٠-٢ دیواره آتش= تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

این تصور اشتباه، بسیار گیج کننده است. چگونه می‌توان بدون اسکن شبکه از نبود تجهیزات بی‌سیم در آن مطمئن شد؟! در محل‌هایی که شبکه‌های LAN بی‌سیم راه‌اندازی نشده‌اند، علاوه بر نقاط دسترسی غیرمجاز، می‌توان از شبکه‌های Ad-Hoc، دسترسی تصادفی لپ‌تاپ‌ها و ایجاد پل‌های ارتباطی با شبکه، به عنوان تهدیدات بالقوه برای امنیت شبکه نام برد. دسترسی تصادفی لپ‌تاپ‌های بی‌سیم یک خطر امنیتی برای صاحبان این لپ‌تاپ‌ها محسوب می‌شود. اگر شرکت مجاور شما از یک نقطه دسترسی بی‌سیم یا یک شبکه Ad-Hoc استفاده می‌کند، احتمال اتصال تصادفی لپ‌تاپ‌های بی‌سیم عضو شبکه شما به این شبکه‌های بی‌سیم زیاد است. این اتصال نوعی خروج از شبکه است. مهاجمان نحوه بهره‌برداری از این شرایط را به خوبی می‌دانند و در نتیجه می‌توانند از یک نقطه دسترسی نرم‌افزاری یا Soft AP (نرم‌افزاری که از روی یک لپ‌تاپ اجرا می‌شود) برای ارسال شناسه‌های SSID موجود روی لپ‌تاپ به یک کامپیوتر خارج از شبکه و حتی ارسال آدرس IP لپ‌تاپ برای کامپیوتر خارجی استفاده کنند. چنان‌که گفته شد، این نقطه ضعف امکان کنترل لپ‌تاپ و حمله به شبکه سیمی را برای مهاجمان فراهم می‌کند. به علاوه، مهاجمان می‌توانند از طریق لپ‌تاپ، حمله‌های MITM (سرنام Man In The Middle) یا سرقت هویت را به اجرا درآورند.

٤-١٠-٣ اسکن دستی= شناسایی تمام نقاط دسترسی غیرمجاز

در این مورد، تلاش مدیران شبکه برای اتخاذ یک رویکرد پیش‌گیرانه به‌منظور شناسایی نقاط دسترسی غیرمجاز در شبکه قابل تقدیر است. اما متأسفانه ابزارهایی که در اختیار این افراد قرار دارد، کارایی لازم را برای شناسایی نقاط دسترسی غیرمجاز ندارد. به‌عنوان مثال، بسیاری از مدیران شبکه از ابزارهای مدیریتی اسکن نقاط ضعف شبکه‌های سیمی به منظور شناسایی نقاط دسترسی غیرمجاز متصل به شبکه استفاده می‌کنند. تجربه‌کاری نگارنده با ابزارهای اسکن نقاط ضعف از هر دو نوع اپن‌سورس و تجاری، بیانگر این است که اغلب مدیران شبکه با تعداد انگشت‌شماری نقطه دسترسی مواجه می‌شوند که توسط سیستم‌عامل شناسایی شده است و هنگامی که شبکه را اسکن می‌کنند، این تجهیزات در قالب یک سیستم مبتنی بر لینوکس همراه یک وب‌سرور شناسایی می‌شوند. هنگام اسکن شبکه‌های Class C و بزرگ‌تر، دستگاه‌های غیرمجاز بین سایر تجهیزات شبکه پنهان شده و نتایج حاصل از اسکن شبکه برای شناسایی نقاط دسترسی غیرمجاز حقیقی نیست.

www.takbook.com

www.takbook.com

کارکرد ابزارهای اسکن بی‌سیم مانند NetStumbler و Kismet بسیار خوب است، اما زمانی که نوبت به شناسایی نقاط دسترسی غیرمجاز می‌رسد، این ابزارها از کارایی لازم برخوردار نیستند. به‌عنوان نمونه این ابزارها نمی‌توانند مشخص کنند که نقاط دسترسی شناسایی‌شده واقعاً به شبکه شما متصل هستند یا خیر. علاوه‌براین، در تعیین موقعیت تقریبی دستگاه بی‌سیم مشکوک نیز دچار مشکل می‌شوند. اگر شرکت شما در یک ساختمان چندطبقه یا یک برج قراردارد، باید امواج دریافتی آنتن‌های بزرگ و دستگاه‌های منتشرکننده سیگنال را نیز به این مشکلات بیافزایید. در چنین شرایطی یک مدیر شبکه با مهارت متوسط در ردگیری و شناسایی تجهیزات بی‌سیم شبکه با مشکلات بزرگی روبه‌رو خواهد شد.

٤-١٠-٤ به‌روزرسانی تمام نقاط دسترسی به‌منظور حذف پروتکل WEP= تأمین امنیت کامل شبکه

پروتکل WEP سالیان دراز مورد حمله مهاجمان قرار گرفته است. علاوه‌براین، براساس اعلان PCI پروتکل WEP باید تا ماه ژوئن سال ۲۰۱۰ به‌طور کامل کنار گذاشته شود. بعضی از شرکت‌ها نیز به سراغ روش‌های توانمندتر کدگذاری و اعتبارسنجی رفته‌اند.

برای جایگزینی این پروتکل، چندگزینه مختلف وجود دارد. متأسفانه بعضی از این گزینه‌ها نیز دارای نقاط ضعف هستند. به‌عنوان مثال، نسخه PSK (سرنام Pre-Shared Key) از پروتکل WPA به دلیل نیاز به انتشار اطلاعات موردنیاز برای ساخت و تأیید کلید رمزگشایی اطلاعات، در مقابل نوعی حمله Offline که روی واژه‌نامه آن انجام می‌شود، آسیب‌پذیر است. برای اجرای این حمله‌ها چندین ابزار مختلف شامل coWPAtty و aircrack-ng وجود دارد. اغلب حمله‌ها شامل گردآوری تعداد زیادی از بسته‌های اطلاعاتی و استفاده از ابزار درمقابل سیستم دریافت بسته‌های اطلاعاتی است. بسته نرم‌افزاری Backtrack 3 تمام ابزارهای لازم را برای اجرای این نوع حمله‌ها فراهم می‌کند. در نوامبر سال ۲۰۰۸ به منظور اثبات این ضعف، پروتکل TKIP هک شد.

در این حمله صرف‌نظر از به‌کارگیری سیستم اعتبار سنجی PSK یا x۸۰۲.۱ مهاجمان توانستند به تمام نسخه‌های پروتکل TKIP شامل WPA و WPA2 نفوذ کنند. با وجود این،کلیدهای TKIP شناسایی نشدند و در نتیجه محتوای تمام قاب‌های کدشده افشا نشد. یک حمله می‌تواند در هر دقیقه یک بایت از داده‌های یک بسته اطلاعاتی رمزنگاری‌شده را افشا کرده و به ازای هر بسته کدگشایی‌شده تا پانزده قاب‌رمزنگاری‌شده را به سیستم تحمیل می‌کند. چنین سیستمی، یک گزینه مناسب برای آلودگی ARP محسوب می‌شود. درک این نکته ضروری است که آن دسته از شبکه‌های WPA و WPA2 که الگوریتم‌های کدگذاری AES-CCMP پیچیده‌تر را مورد استفاده قرار می‌دهند، در برابر حمله‌ها مقاوم‌تر هستند و استفاده از چنین الگوریتم‌هایی به عنوان بهترین رویکرد تدافعی پیشنهاد می‌شود.

www.takbook.com

www.takbook.com

اگر هیچ گزینه دیگری به غیر از راه‌اندازی یک سیستم WPA-PSK پیش رو ندارید، از یک کلمه عبور بسیار مطمئن که حداقل هشت کاراکتر دارد، استفاده کنید. کلمه عبور پیچیده‌ای که از شش کاراکتر تشکیل شده باشد، به‌طور متوسط ظرف سیزده روز کشف می‌شود.

٤-١٠-٥ استفاده از نرم‌افزار کلاینت VPN = محافظت از کارمندان سیار

با وجود این‌که استفاده از برنامه کلاینت VPN همراه یک دیواره آتش نخستین گام برای حفاظت از کارمندان سیار به‌شمار می‌رود، تعداد بسیاری از نقاط ضعف چنین ارتباطی بدون محافظت باقی می‌ماند. کاربرانی که در حال مسافرت هستند، به ناچار در هتل‌ها، کافی شاپ‌ها و فرودگاه‌ها از شبکه‌های وای‌فای استفاده می‌کنند.

ابزارهایی مانند Hotspotter که در بسته نرم‌افزاری BackTrack در اختیار همگان قرار می‌گیرند، برای مهاجم امکان ایجاد یک ناحیه خطرناک را فراهم می‌کنند که اغلب توسط شبکه به‌عنوان یک ناحیه خطرناک مجاز شناخته می شود. این فرآیند شامل ایجاد یک نقطه دسترسی جعلی با استفاده از یک شناسه SSID متداول و همچنین صفحات وب شبیه به یک ناحیه خطرناک واقعی است. سپس مهاجم منتظر اتصال کاربران بی‌اطلاع، به نقطه دسترسی جعلی شده و با استفاده از پروتکل DHCP برای آن‌ها یک آدرس IP و یک صفحه وب ایجاد می‌کند. به این ترتیب، کاربر فریب‌خورده و به‌منظور ورود به ناحیه خطرناک اعتبارنامه خود را در اختیار مهاجم قرار می‌دهد. در بعضی موارد مهاجم حتی دسترسی کاربران به اینترنت را امکان‌پذیر کرده و به این ترتیب برای اجرای حمله‌های MITM و سرقت سایر اطلاعات مهم کاربران مانند شناسه و کلمه عبور و شماره حساب بانکی آن‌ها اقدام می‌کند.

حفاظت از کارمندان سیار به‌ویژه در برابر این نوع حمله‌ها، اقدامی چالش‌برانگیز بوده و علاوه بر استفاده از نرم‌افزار کلاینت VPN و دیواره آتش نیازمند تمهیدات امنیتی دیگری است. البته، هیچ‌یک از این اقدامات به‌طور کامل از کاربر محافظت نمی‌کند، اما خطرات امنیتی را کاهش می‌دهند. مدیران شبکه‌های مبتنی بر ویندوز با استفاده از گزینه Access point (infrastructure) networks only می‌توانند از اتصال کاربران به شبکه‌های Ad-Hoc جلوگیری می‌کنند.

بسیاری از ابزارهای مهاجمان که برای شبیه‌سازی عملکرد نقاط دسترسی به‌کار گرفته می‌شوند، در حقیقت، شبکه‌های Ad-Hock را شبیه‌سازی می‌کنند. غیرفعال‌کردن گزینه مذکور در سیستم‌عامل ویندوز می‌تواند از کاربران در برابر چنین حمله‌هایی محافظت کند. به‌علاوه، غیرفعال کردن گزینه (Any Available Network (Access Point Preferred نیز از بروز چنین حملاتی جلوگیری می‌کند. سرانجام، با

www.takbook.com

www.takbook.com

غیرفعال‌کردن گزینه Automatically Connect to Non-Preferred networks نیز می‌توان از اتصال تصادفی کاربران به شبکه‌های Ad-Hock جلوگیری کرد.

۱۱-٤ جمع‌بندی

در تأمین امنیت شبکه‌های بی‌سیم، به‌کارگیری یک رویکرد چندلایه، کلید اجتناب از بروز مشکلات امنیتی است. درک درست خطرات امنیتی قسمت بزرگی از فرآیند کاهش این خطرات محسوب می‌شود. اغلب حمله‌های بی‌سیم نسبت به لایه دوم شبکه اجرا می‌شوند. بنابراین، بازبینی تنظیمات دیواره آتش فعلی برای حصول اطمینان از فیلترسازی لایه دوم ضروری است. بسیاری از دیواره‌های آتش تنها از لایه سوم و لایه‌های بالاتر حفاظت می‌کنند و بسیاری از آن‌ها نیز به جای نظارت دائمی بر ترافیک اطلاعات به صورت یک فیلتر بسته‌های اطلاعاتی عمل می‌کنند. پیکربندی فیلتر بسته‌های اطلاعاتی می‌تواند به کاری ملال‌آور تبدیل شود. بنابراین، نظارت دائمی بر لایه‌های دوم و سوم شبکه رویکرد مناسب‌تری برای تأمین امنیت شبکه‌های بی‌سیم است.

به‌روزرسانی و تغییر پیکربندی نقاط دسترسی نیز می‌تواند مکمل خوبی برای سیستم‌های کدگذاری و اعتبارسنجی ضعیف باشد. همچنین این اقدامات می‌توانند بسیاری از ملزومات فنی و تکنیکی فعلی و آتی شبکه را تأمین کنند.

بسیاری از حمله‌های امنیتی نیازمند برقراری شرایط خاص هستند و اجرای آن‌ها مستلزم بهره‌مندی از یک سیستم IDS/IPS بی‌سیم برای شبیه‌سازی محیط و تدابیر امنیتی مورد تأیید برای زیرساخت‌های بی‌سیم است. استفاده از یک سیستم IDS/IPS پیشرفته اقدام مؤثری برای شناسایی بسیاری از حمله‌های مذکور و همچنین محافظت در برابر آن دسته از ابزارهای مهاجمان است که برای انجام حمله‌های دنباله‌دار شناخته شده مورد استفاده قرار می‌گیرند. دیواره های آتش به‌هیچ‌وجه قادر به تأمین این نوع امنیت نیستند.

یک سیستم IDS/IPS بی‌سیم ابزارهای بهتری را برای تشخیص نقاط دسترسی غیرمجاز در اختیار ما می‌گذارد. اسکنرهای دستی فقط برای بررسی لحظه‌ای وضعیت شبکه کاربرد دارند و هیچ ابزاری را برای تأمین خودکار امنیت شبکه در برابر نقاط دسترسی غیرمجاز ارائه نمی‌کنند. استفاده از یک سیستم IDS/IPS بی‌سیم به منظور نظارت شبانه‌روزی بر شبکه و نابودی خودکار نقاط دسترسی غیرمجاز رویکرد کارآمدتری برای کاهش خطرات امنیتی شبکه محسوب می‌شود. به‌علاوه، این رویکرد موجب صرفه‌جویی در زمان طولانی موردنیاز برای نظارت و بررسی دستی شبکه می‌شود.

www.takbook.com

www.takbook.com

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.

www.takbook.com

www.takbook.com

۵ فصل پنجم:پروتکل های امنیتی در شبکه های وای فای

Chapter FIve:Security Protocols in Wi-Fi Networks

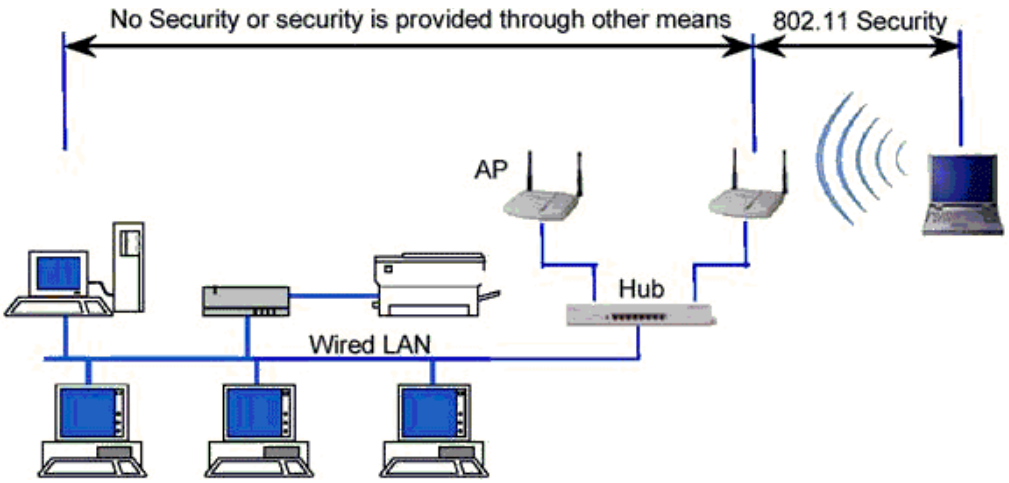
مراجع:[11],[12],[13],[14],[15],[16]

www.takbook.com

www.takbook.com

۵-۱ مقدمه

این فصل به بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۸۰۲.۱۱ سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل(WEP (Wired Equivalent Privacy تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان کلاینت ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد ۸۰۲.۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



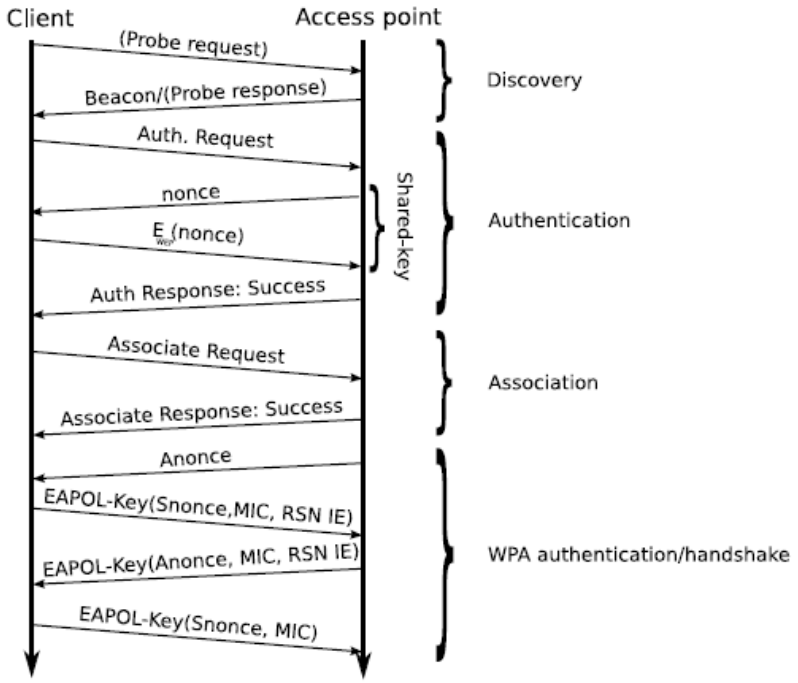
شکل ۵.۱:محدودیت های استاندارد های امنیتی ۸۰۲.۱۱ خصوصا WEP

۵-۲ پروتکل اتصال/دسترسی در شبکه های وای فای

شکل ۵.۱ روند جریان مبادله فریم ها برای اتصال یک کلاینت به نقطه دسترسی را نشان می دهد،که در تمامی پروتکل ها از روند استفاده می شود.

www.takbook.com

www.takbook.com



شکل ۵.۱ :پروتکل اتصال به شبکه های وای فای

در این روند یک کلاینت برای اتصال به شبکه های وای فای ابتدا با ارسال یک فریم به نامProbe Request و دریافت فریم ProbeResponse از جانب نقطه دسترسی یا به وسیله فریم هایی به نام Beacon که مکررا از نقطه دسترسی به تمام ایستگا ههـا ارسـال مـی شـود،نقطه دسترسـی را شناسـایی مـی کند.بعـد از شناسایی نقطه دسترسی،کلاینت باید خودش را به نقطه دسترسی شناسایی کرده و عملیات احراز هویـت را انجام دهد و اگر توانست خودش را به نقطه دسترسی شناسایی کند و بـا موفقیـت احـراز هویـت را انجـام دهد،آنگاه سعی می کند که به نقطه دسترسی وصل شود و با ارسال فریم هایی به نـام association request به نقطه دسترسی درخواست وصل شدن می کند و در صورتی که نقطه دسترسـی موافقـت کنـد بـا ارسـال فریمی به نام positive association response به کلاینت اجازه اتصال می دهد،اگر WPA فعال باشد روش احراز هویت کلید اشتراکی که در پروتکل WEP به کار می رود استفاده نمی شود و از احراز هویت واقعـی به جای ان استفاده می شود.

بعد از انجام چهار مرحله بالا کلاینت می تواند به دریافت و ارسـال و مبادلـه فـریم بـا نقطـه دسترسـی بپردارد

۵-۳ قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه هـای بـی‌سـیم بـر اسـاس استاندارد ۸۰۲.۱۱ فراهم می‌کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نـوع اسـتفاده از آن

www.takbook.com

www.takbook.com

همواره امکان نفوذ به شبکه های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی کلاینت ها و سخت‌افزارهای بی‌سیم، خصوصاً کلاینت های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه های سیمی و بی‌سیم‌یی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد :

- Authentication
- Confidentiality
- Integrity

احراز هویت(Authentication)

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

محرمانگی (Confidentiality)

محرمانه گی هدف دیگر WEP است. این بُعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

www.takbook.com

www.takbook.com

صحت(Integrity)

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان کلاینت های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.

۵-٤ خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲.۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد ۸۰۲.۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می‌نماید. سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۸۰۲.۱۱ دو گونه خدمت هویت سنجی را تعریف می‌کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سّری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترک و با بهره‌گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می‌نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.

www.takbook.com

www.takbook.com

در یک شبکه بی‌سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک داده ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه‌های سیمی نماید.

۵-٤-۱ احراز هویتAuthentication

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.جزئیات این روش در فصل ۵ و در قسمت به طور کامل بیان گردیده است و از تکرار مجدد آن خودداری می کنیم.(رجوع شود به ۳-۵-۱)

۵-٤-۲ سرویس امنیت (confidentialityیاPrivacy)

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.

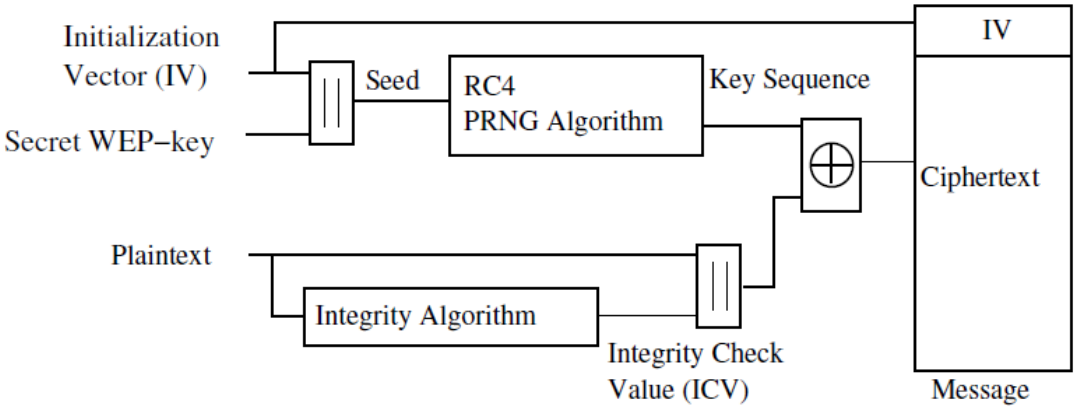
در استاندارد ۸۰۲.۱۱b، از تکنیک های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به بیان دیگر داده های تمامی لایه های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست های امنیتی در شبکه های محلی بی‌سیم مبتنی بر استاندارد ۸۰۲.۱۱b است، معمولاً به کل پروسه‌ی امن سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود.

در شکل زیر بلوک دیاگرام رمزنگاری پروتکل WEP را مشاهده می کنید، WEP از الگوریتم RC4 PRNG برای تولید یک عدد شبه تصادفی استفاده می کند،تمام ایستگاها از یک کلید اشتراکی به نام Secret WEP-Key استفاده می کنند،در مجموع برای انجام عملیات رمز نگاری یک مقدار اولیه(IV) به کلید اصلی

www.takbook.com

www.takbook.com

الحاق می گردد و به عنوان ورودی برای الگوریتم RC4 PRNG به کار می رود ،خروجی این الگوریتم دنباله ای از کلید ها می باشد ،متن خام ورودی توسط الگوریتم Integrity به یک مقدار تست کننده صحت (ICV)،تبدیل می شود و به متن خام اصلی اضافه می شود و سپس با دنباله کلید تولید شده XOR می شود و خروجی به عنوان Payload در فریم داده قرار می گیرد،برای عملیات رمزگشایی بسته عکس عملیات رمزنگاری در فرستنده انجام می شود تا داده ای بسته به دست آیند.



شکل ۵.۲ :بلوک رمزنگاری پروتکل WEP

همان طور که گفته شد پروتکل WEP سرویس های امنیتی محرمانگی،احراز هویت و کنترل دسترسی را فراهم می کند ،اما می توان روش های به کار برد که این سرویس ها را از میان برداشت و بتوان به شبکه های وای فای نفوذ کرد،در زیر روش هایی که می تواند این سرویس ها را بشکند و به پروتکل حمله کنند.

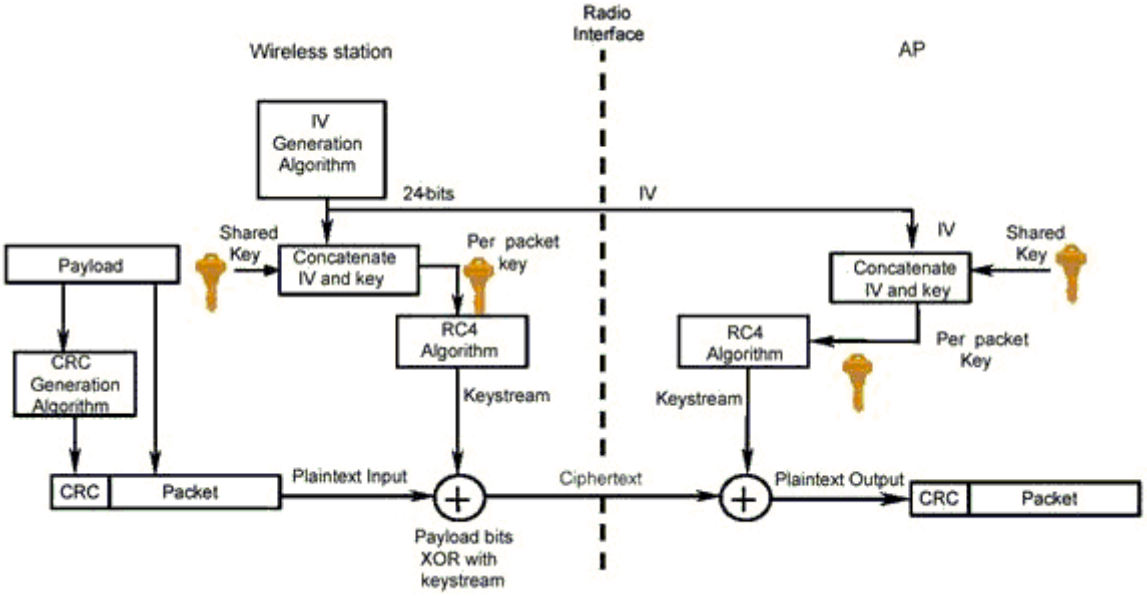
کلیدهای WEP اندازه هایی از ٤٠ بیت تا ١٠٤ بیت می‌توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ٢٤ بیتی ترکیب شده و یک کلید ١٢٨ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ٨٠ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ٨٠ بیت (که تعدد آن‌ها از مرتبه‌ی ٢٤ است) به اندازه‌یی بالاست که قدرت پردازش سیستم های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه های محلی بی‌سیم از کلیدهای ٤٠ بیتی برای رمزکردن بسته های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این ست که روش تأمین محرمانه گی 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.

www.takbook.com

www.takbook.com

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل ۵.۳ نمایش داده شده است :



شکل ۵.۳ :عملیات الگوریتم WEP برای تضمین محرمانگی

۵-٤-۳ صحت (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 ۸۰۲.۱۱ b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان کلاینت های 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 به‌معنای 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 ۸۰۲.۱۱ b 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

www.takbook.com

www.takbook.com

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 شبکه های بی‌سیم ندارد. این مشکل از شبکه های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخ‌داد چنین سهل‌انگاری‌هایی، زمانی که تعداد کلاینت های شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

۵-۵ ضعف‌های اولیه‌ی امنیتی WEP

در این قسمت به بررسی ضعف های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.همان گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد ۸۰۲.۱۱ بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ٤٠ 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 ١٠٤ 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 همان طور که در قسمت های 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

۲. Initialization Vector –IV

۳.ضعف در الگوریتم

۳. استفاده از CRC رمز نشده

www.takbook.com

www.takbook.com

۵-۵-۱ 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 کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۵-۵-۲ Initialization Vector – IV

این بردار که یک فیلد ٢٤ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان دهنده‌ی 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 شبکه های 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 داده های رمز شده‌ی شبکه بپردازد و IVهای بسته های 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.

۵-۵-۳ ضعف در الگوریتم

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

www.takbook.com

www.takbook.com

۵-۵-٤ استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دست‌رسی بی‌سیم به سوی 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 ۵.۱ ضعف‌های امنیتی پروتکل WEP را به‌اختصار جمع‌بندی کرده است:

www.takbook.com

www.takbook.com

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.

جدول ۵.۱ : ضعف های امنیتی استاندارد WEP

لیستی ار انواع حملات به شبکه های وای فای به همراه سرویسی را که به مخاطره می اندازد و نیازمندی ها و زمان مورد نیاز را مشاهده می کنید:

Attack	Service	Requirements	Approximate Time
RC4	Confidentiality, Authentication	300,000 WEP encrypted frames	20 minutes
WEP dictionary	Confidentiality, Authentication	Pass-phrase seeded key, 1 data frame	Norwegian word list in 5 sec.
Chosen plaintext	Confidentiality	WEP enabled. Allow 10 byte data size	50 minutes for full frame
Redirect	Confidentiality	WEP enabled	Insignificant
Double encryption	Confidentiality	Internet connection	At least a few hours
One way auth	Authentication	Shared-key authentication	Insignificant
Spoofing	Authentication	1 active and authenticated client	Insignificant
Rogue access point	Authentication	1 client	Insignificant
Packet injection	Access control	Known IV/key sequence	Insignificant
Profiling	Access control	Known IV/key sequence	Insignificant
MAC filter	Access control	MAC filter enabled	Insignificant
Captive Portal	Access control	MAC filter access control	Insignificant
WPA-PSK dictionary	Confidentiality, Authentication	Pass-phrase seeded key, handshake	Norwegian word list in 1 hour

www.takbook.com

www.takbook.com

با وجود اینکه نفوذگران مصمم، می توانند در WEP نفوذ نمایند، استفاده از WEP می تواند مانع از جداکردن داده های بی سیم شناور اطراف شبکه تان توسط بسته های نظارت و ردگیری (اسنیفر پاکت ها) شود (یکی از قدیمی ترین روش های سرقت اطلاعات در یک شبکه، استفاده از فرآیندی موسوم به "ردگیری بسته ها در شبکه" است. در این روش مهاجمان از تکنیک هایی به منظور تکثیر بسته های اطلاعاتی که در طول شبکه حرکت می کنند، استفاده نموده و در ادامه با آنالیز آنها از وجود اطلاعات حساس در یک شبکه آگاهی می یابند.

امروزه پروتکل هائی نظیر IPSec به منظور پیشگیری از "ردگیری بسته ها در شبکه" طراحی شده است که با استفاده از آن بسته های اطلاعاتی رمزنگاری می گردند. در حال حاضر تعداد بسیار زیادی از شبکه ها از تکنولوژی IPSec استفاده نمی نمایند و یا صرفاً بخش اندکی از داده های مربوطه را رمزنگاری می نمایند و همین امر باعث شده است که "ردگیری بسته ها در شبکه"همچنان یکی از روش های متداول به منظور سرقت اطلاعات باشد. یک "ردگیر بسته ها در شبکه" که در برخی موارد از آن به عنوان دیده بان شبکه و یا تحلیلگر شبکه نیز یاد می شود، می تواند توسط مدیران شبکه به منظور مشاهده و اشکال زدائی ترافیک موجود بر روی شبکه استفاده گردد تا به کمک آن بسته های اطلاعاتی خطاگونه و گلوگاه های حساس شبکه شناسائی و زمینه لازم به منظور انتقال موثر داده ها فراهم گردد. به عبارت ساده تر، یک "ردگیر بسته ها در شبکه" تمامی بسته های اطلاعاتی که از طریق یک اینترفیس مشخص شده در شبکه ارسال می گردند را تا موقعی که امکان بررسی و آنالیز آنان فراهم گردد جمع آوری می نماید. عموماً از برنامه های "ردگیر بسته ها در شبکه" به منظور جمع آوری بسته های اطلاعاتی به مقصد یک دستگاه خاص استفاده می شود. برنامه های فوق قادر به جمع آوری تمامی بسته های اطلاعاتی قابل حرکت در شبکه، صرف نظر از مقصد مربوطه نیز هستند. یک مهاجم با استقرار یک "ردگیر بسته ها در شبکه" در شبکه، قادر به جمع آوری و آنالیز تمامی ترافیک شبکه خواهد بود. اطلاعات مربوط به نام و رمز عبور عموماً به صورت متن معمولی و رمز نشده ارسال می شود و این بدان معنی است که با آنالیز بسته های اطلاعاتی، امکان مشاهده اینگونه اطلاعات حساس وجود خواهد داشت. یک "ردگیر بسته ها در شبکه" صرفاً قادر به جمع آوری اطلاعات مربوط به بسته های اطلاعاتی درون یک subnet مشخص شده است. بنابراین، یک مهاجم نمی تواند یک "ردگیر بسته ها در شبکه" را در شبکه خود نصب نماید و از آن طریق به شبکه شما دستیابی و اقدام به جمع آوری نام و رمز عبور به منظور سوء استفاده از سایر ماشین های موجود در شبکه نماید. مهاجمان به منظور نیل به اهداف مخرب خود می بایست یک "ردگیر بسته ها در شبکه" را بر روی یک کامپیوتر موجود در شبکه اجراء نمایند). در بیشتر نقاط دسترسی، پیشنهاد می کنند حداقل اندازه کلید برای رمزگذاری ٦٤ بیت باشد و بعضی دیگر حتی پیشنهاد ۱۲۸ بیتی برای رمزگذاری را داده اند. مدلWEP بسته های داده های مورد استفاده را بصورت الگوریتم های مبهم و مبتنی بر یک کلید

www.takbook.com

www.takbook.com

الکترونیکی تبدیل نموده و آنرا بصورت یک سری از الفبای عددی یا کاراکترهای شانزده شانزدهی (هگزا دسیمال) پنهان می نماید. سیستم دریافت باید یک کلید نظیر آن را به منظور کشف رمز بسته داده داشته باشد.

بر روی نقطه دسترسی، گزینه ای را که اتصال WEP را فعال نموده و یا نیاز دارد، جستجو کنید. کلیدی را روی نقطه دسترسی تعریف نموده و همان کلید را در پیکربندی بی سیم هر سرویس گیرنده وارد کنید.

۵-۶ پروتکل WPA(Wi-Fi Protected Access)

اتحادیه Wi-Fi در سال ۲۰۰۳ استاندارد جدیدی را برای شبکه‌های بی‌سیم معرفی کرد. این استاندارد برای به کار گیری در ابزارهای شبکه موجود که از استاندارد WEP استفاده می کردند، طراحی شد و از قابلیت سازگاری با ابزارهای قدیمی تر نیز برخوردار است. به کارگیری این استاندارد مستلزم پیکربندی آن روی ابزارهای موجود در شبکه بوده و در صورتی که تنظیمات مورد نظر روی دستگاهی اعمال نشود همچنان رمزگذاری اطلاعات بر اساس استاندارد WEP انجام می شود. مهم ترین ویژگی این استاندارد که آن را نسبت به WEP متمایز می کند، قابلیت تغییر کلید به صورت دینامیک با استفاده از پروتکل TKIP (Temporal Key Integrity) است. این استاندارد برای رمز گذاری اطلاعات از الگوریتم MIC (Message Integrity Check) استفاده می‌کند و با افزودن ویژگی بررسی کامل کلید، اطمینان می‌یابد که کلید تعریف شده مورد استفاده کاربران غیر مجاز قرار نخواهد گرفت.

پروتکل TKIP (Temporal Key Integrity Protocol) به این منظور در پروتکل WPA به وجود آمد که بتواند ضعف‌های امنیتی ناشی از الگوریتم RC4 در پروتکل WEP را جبران کند. یکی از مهم‌ترین برتری‌های WPA بر WEP این است که در آن هر بسته با استفاده از یک کلید منحصر به فرد و متفاوت با بسته قبل رمزنگاری می‌شود و این کار توسط پروتکل TKIP انجام می‌گردد. پروتکل TKIP به جای استفاده مستقیم از کلید مشترک برای رمزنگاری از آن تنها برای تولید سایر کلیدها استفاده می‌کند. این پروتکل دو تابع ترکیب کلید دارد که این توابع از ترکیب کلید مشترک، آدرس MAC سرویس‌گیرنده و بردار اولیه، به ازای هر بسته یک کلید را تولید می‌کنند. با استفاده از TKIP، کلید رمزنگاری به جای یک کلید ٦٤ یا ۱۲۸ بیتی که تنها ۲٤ بیت آن پویا است (کلید مشترک مورد استفاده در WEP) به یک کلید پویای ۱۲۸ بیتی کاملاً مؤثر تعییر می‌کند و در نتیجه امنیت شبکه‌ی بی‌سیم افزایش می‌یابد.

برای رمز گذاری شبکه بر اساس استاندارد WPA، یک ترکیب منحصر به فرد از کلید تعریف شده به همراه SSID شبکه ایجاد شده و به هر کاربر شبکه بی‌سیم به صورت مجزا اختصاص می‌یابد که به طور

www.takbook.com

www.takbook.com

ثابت و اتوماتیک تغییر می یابد در نتیجه امکان دسترسی افراد غیر مجاز به شبکه را به حداقل می رساند. قابلیت شناسایی کاربران که در استاندارد WEP نادیده گرفته شده بود، در این استاندارد و به کمک پروتکل EAP (Extensible Authentication Protocol) تامین شد. در حقیقت WEP دسترسی کاربران را بر اساس آدرس MAC کامپیوترهای شبکه تنظیم می کرد که به راحتی توسط هکرها قابل شناسایی بود. EAP بر پایه یک سیستم کلید عمومی ایمن تر ساخته شده است تا دسترسی به شبکه را تنها برای کاربران واجد شرایط و شناسایی شده فراهم کند.

در شبکه‌ای که از پروتکل WPA استفاده می‌شود، در ابتدا یک میزبان با نقطه دسترسی ارتباط برقرار می‌کند. تا هنگامی که هویت کاربر تصدیق نشده است، نقطه دسترسی از دسترسی کاربر به شبکه محلی جلوگیری می‌کند. اگر هویت کاربر توسط سرویس‌دهنده احراز هویت تصدیق شود، میزبان می‌تواند به شبکه محلی ملحق شود. در غیر این صورت از دسترسی میزبان به شبکه جلوگیری می‌شود. پس از ملحق شدن میزبان به شبکه محلی، سرویس‌دهنده تصدیق هویت، یک کلید رمزنگاری TKIP میان میزبان و نقطه دسترسی توزیع می‌کند. سپس میزبان می‌تواند ارتباط خود را روی شبکه محلی آغاز کرده و داده‌ها را به صورت رمزنگاری شده منتقل کند.

WPAمخفف دسترسی محافظت شده Wi-Fi یا Wi-Fi Protected Access می باشد و عبارتست از استانداردهایی که برای افزایش ویژگی های امنیتی WEP طراحی شده است. این تکنولوژی به گونه ای طراحی شده است که بتوان از آن در دستگاه های موجود که از Wi-Fi پشتیبانی کرده و دارای سیستم امنیتی WEPهستند، استفاده نمود. (به عنوان مثال از طریق بروزرسانی نرم افزار این دستگاه ها..)

این تکنولوژی نسبت به WEP دارای دو مزیت است :

- رمزنگاری داده پیشرفته تر با استفاده از پروتکل TKIP. این پروتکل کلیدهای رمزنگاری را با استفاده از الگوریتم Hashing به هم ریخته و با افزودن کد بررسی پیوستگی به آن از عدم جعل کلید توسط هکرها اطمینان حاصل می نماید.
- تایید هویت کاربران با استفاده از پروتکل EAP، این ویژگی در تکنولوژی WEP به عنوان یک نقیصه بشمار می آمد.WEP دسترسی به شبکه های بی سیم را بر اساس آدرس MAC کامپیوترها کنترل می نماید و از آنجا که آدرس MAC به راحتی قابل شناسایی و استفاده توسط هکرها می باشد، روش مناسبی به شمار نمی آید. پروتکل EAP بر اساس کلید رمزنگاری عمومی بسیار ایمن تر عمل نموده و بر این اساس تنها کاربران تایید شده قادر به دسترسی به شبکه خواهند بود.

اگر بخواهیم مقایسه بین پروتکل های WEP و WPA داشته باشیم می توان گفت که پروتکل WEP در کمتر از ده دقیقه درهم شکسته می شود، اما درهم شکستن WPA با یک کلید ۲۱ بیتی بیشتر از ٤ × ۱۰۲۰

www.takbook.com

www.takbook.com

سال طول می کشد WEP .تنها مـی توانـد از کلیـدهای ٦٤، ١٢٨ و ١٥٢ بیتـی و یـک IV (Initialization Vector)یکسان یا همان بردار تولید کلیدهای ابتدایی رمزنگاری استفاده کند، امـا در WPA از دو الگـورتیم رمزنگاری پیچیده به نـام هـای TKIP سـرنام (Temporal Key Integrity Protocol) و AES (Advanced Encryption Standard)استفاده می شود که در هر کدام کلیـدها ده هـا بـار تولیـد شـده و در رمزنگـاری اطلاعات شرکت کرده و از بین می روند. طول بردار IV دو برابر WEP است. IV در WPA قابلیت تعریـف پانصد تریلیون کلید مقایسه را فراهم می کند، اما این تعداد در WEP نزدیک به ١٦/٧ میلیـون کلیـد مقایسـه است.

در پروتکل WEP برای تولید کد صحت پیام از روش CRC (جمع تطبیقی) استفاده می‌شود که یک تابع خطی ساده است، در حالی که پروتکل WPA از الگوریتم Michael برای محاسبه‌ی کد صحت پیام (MIC) استفاده می‌کند که یک تابع بسیار پیچیده است. تفاوت دیگر کد صحت پیام محاسبه شـده در پروتکـل‌هـای WEP و WPA این است که در پروتکل WEP کد CRC فقط از روی قسمت اصلی بسته-ی داده محاسـبه می‌شود و کاری به سرآیند بسته ندارد، در حالی که پروتکل WPA از کل داده‌ها (داده‌های اصلی با اضـافه‌ی سرآیند) برای محاسبه‌ی کد MIC استفاده می‌کند. بنابراین، در پروتکل WEP ممکن است اطلاعات سـرآیند بسته (از قبیل آدرس فرستنده، آدرس گیرنده و غیره) در حین ارسال دچار تغییر شوند بدون این که گیرنـده متوجه شود.

اما دلیلی که هنوز دیده می شود که از پروتکل WEP استفاده می شود این است کـه بسـیاری از دسـتگاه های بی سیم امروزی هنوز از WPA و نسخه های جدیدتر آن پشتیبانی نمی کنند و تنها گزینه امنیتی آن هـا WEP است. بسیاری از کارت های شبکه بی سیم قدیمی، بسیاری از دستگاه هـای بـازی ماننـد Nintendo DS و نوت بوک های قدیمی فقط از WEP پشتیبانی می کنند. همچنین نمـی تـوان گفـت کـه تحـت هـیچ شرایطی از WEP استفاده نکنید، بلکه که WPA بهتـر از WEP اسـت و WEP بهتـر از رمزنگـاری نکـردن اطلاعات روی شبکه های بی سیم است. اگر در شبکه دستگاه بی سیمی دارید کـه از WPA پشـتیبانی نمـی کند، ناچارید از WEP استفاده کنید. بالاخره هر فردی نمی تواند به سادگی رمزنگاری ایـن پروتکـل را دور بزند.

۵-۷ پروتکل WPA2

WPA2 مخفف دسترسی محافظت شده به Wi-Fi ویرایش دوم یا "Wi-Fi Protected Access 2" مـی باشد، که این پروتکل در جهت بهبود پروتکل WPA که در شبکه های بـی سـیم کـاربرد دارد ، ارایـه شـده است. این پروتکل در کنترل شبکه وحفاظت داده ها بسیار قوی تر عمل نمـوده و اسـتفاده از ایـن پروتکـل

www.takbook.com

www.takbook.com

درشبکه های بی سیم شرکت های بزرگ و کاربران خانگی سطح بسیار بالایی از امنیت را فراهم کرده و کاربران این پروتکل می توانند ازجلوگیری از دسترسی غیر مجاز به شبکه خود اطمینان داشته باشند.

بر اساس استاندارد IEEE 802.11i، WPA2 با بکار گیری استانداردها FIPS 140-2 متعلق به موسسه استاندارد سازی و تکنولوژی ایالات متحده (NIST) به همراه الگوریتم رمزنگاری AES و همچنین روش تایید هویت موجود در استاندارد های ۸۰۲.۱ می تواند امنیت داده را هم تراز با استانداردهای دولتی ایالات متحده فراهم نماید.

این استاندارد نسخه کامل تر استاندارد WPA است که در سال ۲۰۰٤ تعریف شد و مهم‌ترین تفاوت این دو استاندارد در نحوه رمزگذاری اطلاعات برای ارسال به مقصد می باشد. WPA2 یا استاندارد ۸۰۲.۱۱ i که قوی‌ترین استاندارد رمزگذری شبکه های بی‌سیم است و پس از WPA ارایه شد، از یک سیستم با نام AES (Advanced Encryption Standard) بهره می‌گیرد که موجب می‌شود شکستن کلید رمز به راحتی امکان‌پذیر نباشد. WPA2 در دو نسخه پیاده‌سازی می‌شود: WPA2-Personal و WAP2-Enterprise. WPA2-Personal که با نام WPA-PSK شناخته می‌شود برای استفاده در شبکه‌هایی با کاربران محدود مانند دفاتر اداری کوچک و خانه ها طراحی شده است. این استاندارد دسترسی غیرمجاز به شبکه را با استفاده از تنظیم رمز عبور غیرفعال خواهد کرد و دسترسی هر دستگاه بی سیم با استفاده از یک کلید ۲٥٦ بیتی به منابع شبکه امکان‌پذیر خواهد بود. نسخه WAP2-Enterprise یا WPA-802.1X، برای استفاده در موسسات و سازمان‌ها مورد استفاده قرار می‌گیرد و کاربران از طریق سرور به شبکه دسترسی خواهند یافت. پیاده‌سازی این استاندارد به تنظیمات پیچیده‌تری نسبت به سایر استانداردها نیاز دارد اما امنیت بالاتری را برای شبکه‌ای با تعداد کاربران متعدد فراهم خواهد کرد.

کارشناسان شبکه توصیه می‌کنند در صورتی که ابزار بی‌سیم مورد استفاده در شبکه شما از استاندارد WEP پشتیبانی می کنند بدون اتلاف وقت به سراغ استانداردهای قوی‌تر و مطمئن‌تر رفته و امنیت شبکه بی سیم خود را به سرعت ارتقا دهید، زیرا عدم استفاده از استاندارد رمزگذاری و یا به‌کارگیری WEP هر دو تقریبا به یک معنا است و این شرایط تفاوت چشم گیری با یکدیگر نخواهند داشت.در حال حاضر بهترین و کارآمدترین استاندارد رمزگذاری، WPA2 است و تقریبا می‌توان گفت امروزه تمامی محصولات شرکت‌های فعال در حوزه ابزارهای شبکه‌سازی بی‌سیم قابلیت پشتیبانی از استاندارد رمزگذاری WPA2 را دارند بنابراین به شما توصیه می کنیم برای برقراری امنیت اطلاعات و همچنین جلوگیری از دسترسی افراد غیر مجاز به شبکه در صورتی که ابزار بی‌سیمی که مورد استفاده قرار می‌دهید، قابلیت پشتیبانی از این استاندارد را دارد از WPA2 استفاده کنید.

www.takbook.com

www.takbook.com

WPA یک پروتکل به روزتر و سازگارتر با استاندارد 802.11 n است و از متدهای رمزنگاری و امن کردن اطلاعات برای انتقال توسط امواج استفاده می کند که تا کنون هیچ کس نتوانسته آن را شکسته و رمزگشایی کند. نسخه های WPA2 و WPA2 Enterprise نسخه های جدیدتری نسبت به WPA هستند و به یقین از الگوریتم ها و روش های بهتر رمزنگاری استفاده می کنند. اگر روتر یا نقطه دسترسی شما از WPA2 یا WPA2 Personal پشتیبانی می کند، این گزینه را انتخاب کنید. در غیر این صورت WPA ساده نیز بهترین انتخاب برای رمزنگاری داده های بی سیم است.

پروتکل WPA2 از الگوریتم رمزنگاری AESاستفاده می‌کند، در حالی که پروتکل WPA از پروتکل TKIP استفاده می‌کند ولی الگوریتم رمزنگاری آن همان الگوریتم RC4 استفاده شده در پروتکل WEP است. تفاوت دیگر پروتکل‌های WPA و WPA2 در روش محاسبه کد صحت پیام (MIC) می‌باشد. پروتکل WPA برای تولید کد صحت پیام از الگوریتم Michael استفاده می‌کند ولی پروتکل WPA2 از شیوه‌ی زنجیره‌سازی بلوک‌های رمز (CBC)* برای تولید کد صحت پیام استفاده می‌کند. با وجود پیچیده بودن الگوریتم Michael، روش CBC به کار گرفته شده در پروتکل WPA2 برای محاسبه‌ی کد صحت پیام دارای پیچیدگی بیشتر بوده و در نتیجه امنیت بیشتری را تأمین می‌کند.

۵-۸ پروتکل امنیتی WPS

Wi-Fi Protected Setup یا راه‌اندازی حفاظت شده Wi-Fi (به اختصار WPS) استانداردی است برای پیاده سازی شبکه‌های بی سیم خانگی به شکلی امن و آسان است. این استاندارد در ۸ ژانویه ۲۰۰۷ توسط اتحادیه Wi-Fi به صورت رسمی تایید شد.

هدف این استاندارد تسهیل در روند پیکربندی امنیتی شبکه های بی سیم می‌باشد و به همین دلیل است که قبلا با نام Wi-Fi Simple Config نامیده می‌شد. این پروتکل به منظور میسر کردن امنیت برای کاربرانی طراحی شده که اطلاعات کمی در مورد امنیت شبکه های بی سیم دارند و ممکن است درمیان گزینه‌های موجود برای ایجاد امنیت در شبکه‌های بی سیم سردرگم بمانند.

این استاندارد با تمرکز بر امنیت و قابلیت استفاده آسان چهار روش برای شبکه های خانگی فراهم می‌کند، که عبارتند از:

روش PIN: در این روش باید یک PIN (کد شناسایی شخصی) از روی برچسب نصب شده روی دستگاه و یا صفحه نمایش (در صورت وجود) خوانده شده و درنقطه دسترسی (AP) ثبت گردد .این متد روش پایه در نظر گرفته می شود و بر این اساس می بایست در تمامی تجهیزاتی که دارای گواهینامه این استاندارد می‌باشند الزاما وجود داشته باشد.

www.takbook.com

www.takbook.com

روش PBC: در این روش لازم است که کاربر به سادگی یک دکمه فیزیکی یا مجازی را بر روی هر یک از دو نقطه شاملنقطه دسترسی و دستگاهی که می خواهد بانقطه دسترسی ارتباط امن داشته باشد، بفشارد. پشتیبانی از این روش براینقطه دسترسی ها اجباری ولی برای دستگاه‌های بی سیم دیگر اختیاری می باشد.

روش NFC: در این روش فقط کافیست که کاربر دستگاه مورد نظر را نزدیکنقطه دسترسی قرار دهد تا امکان یک ارتباط میدانی کوتاه بردبین این تجهیزات برقرار شود. بجای این کار، بهره بردن از برچسب های RFID سازگار نیز امکان‌پذیر می‌باشد. پشتیبانی از این روش اختیاری است.

روش USB:در این روش کاربر از یک حافظه USB(USB Stick) برای انتقال داده بین دستگاه ونقطه دسترسی استفاده می نماید. پشتیبانی از این روش اختیاری است.

از دو روش آخر غالباً به عنوان روش‌های خارج از باند "Out Of Band" یاد می‌شود، چراکه انتقال اطلاعات در این دو روش نیاز به راه حلی به غیر از استفاده از خود شبکه Wi-Fi دارد.

به خاطر داشته باشید که در حال حاضر برای اعطای گواهینامهاین استاندارد فقط دو روش اول لحاظ می‌گردد و روش USB نیز از رده خارج شده محسوب گردیده و از روند اعطای گواهینامه خارج شده است.

مزایا

۱. پیکربندی خودکار نام شبکه(SSID) و کلید امنیتی (WPA) بر روی دستگاه و نقطه دسترسی

۲. عدم نیاز به دانستن نام شبکه(SSID) ، کلیدهای امنیتی و گذرواژه‌ها در هنگام اتصال به شبکه‌های دارای WPS

۳. پایین بودن احتمال اینکه گذرواژه‌ها و کلیدهای امنیتی قابل حدس زدن باشند، زیرا که به صورت تصادفی تولید می‌شوند.

۵-۹ جمع بندی

امروزه روش های زیادی برای امن کردن شبکه های بی سیم وجود دارد که هر کدام ضعف ها و سختی های خاص خود را دارد ولی این باعث نشده است که شبکه های بی سیم پیش رفت روز افزون خود را به دست نیاورند. به همین دلیل فراهم کردن شبکه ای بی سیم و امن یکی از تخصص های پول ساز می باشد.

www.takbook.com

www.takbook.com

٦ مشکلات فعلی و کارهای آتی

روش ها و پروتکل های امن سازی در شبکه های وای فای بررسی شد و نقاط قوت و ضعف هریک از روش ها بررسی شد، همچنین چالش ها و نقاط ضعف امنیتی این شبکه ها و راه حل آنها نیز اشاره شد. اما همچنان برای امن سازی این شبکه ها نیاز به روش های بهتر و بهینه تر نیاز می شود در زیر لیستی از کار هایی که باید برای امنیت بیشتر در این شبکه ها کار شود و به عنوان مسائل باز مطرح می شود را بیان می کنیم:

۱. **حملات منع سرویس:**حملات منع سرویس (Denail Of Service) یکی از معروفترین حملاتی است که در چند سال اخیر امنیت تمام شبکه را تهدید کرده است، در این حملات هکر قصد دارد که با حمله کردن به سرور و شبکه آن را از کار انداخته و مانع انجام روال های عادی و سرویس دهی آن شود.این حملات در شبکه های وای فای نیز به طور جدی مطرح است و حتی به می توان گفت با توجه به ماهیت این شبکه ها، شدید تر نیز می باشد ،پروتکل های که در این تحقیق معرفی شدنمی توانند جلوی این حمله را بگیرند و در نتیجه نیاز به اصلاحاتی در این پروتکل ها یا ارائه پروتکل های جدیدتر برای مقابله با این حملات می باشم.

۲. پروتکل های WPA WEP :همانطور که بررسی شد این پروتکل ها به عنوان پروتکل های غالب برای تامین امنیت در شبکه های وای فای محسوب می شوند و از طرفی مشکلات این پروتکل ها نیز بررسی شد و همانطور که گفته شد این پروتکل ها امنیت را تا سطحی تامین می کنند و هیچ وقت قادر به تامین امنیت کامل نمی باشند و ازطرفی برای بهینه شدن نیاز به تغییراتی دارند و ایده های نو می تواند کارایی و عملکرد این پروتکل ها را افزایش دهد.

www.takbook.com

www.takbook.com

مراجع

[1] “Wi-Fi Security How to Break and Exploit”, Thesis for the degree Master of Science Hallvar Helleseth Department of InformaticsUniversity of Bergen June 2006

[2]" An Introductionto Wi-Fi®”, Part Number 019-0170 • 090409–B • Printed in U.S.A.Digi International Inc. © 2007-2008

[3] IEEE 802.11 Working group website ,http://www.ieee802.org/11

[4] Introduction to IEEE 802.11"",intellgraphics",http://www.intellgraphics.com"

[5] steve Kapp,"802.11:Leaving the wire behind ",IEEE internet computing ,January-February 2002,pp.82-85

[6] steve Kapp "802.11a :More bandwidth without the wire ",IEEE internet computing ,Julay-Aguest 2002,pp.75-79

[7] Edgar Danielyan "IEEE 802.11 ",the internet Protocol Journal ,Vol.5,No.1,March2002,pp.2-13

[8] "A condensed review of Spread Spectrum Techniques for ISM band System ",Intersil Application Note,AN9820.1,May 2000

[9]" Wi-Fi Security"Stewart S. Miller,McGraw-Hill-New York Chicago San Francisco Lisbon London Madrid Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Toronto

[10] بانک مقالات گروه امداد امنیت کـامپیوتری ایـران (Iran Computer Emergency Response Team - CERT)

[11] “Overview of Wi-Fi Security What is left?”,Philippe Teuwen,Security Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group,N.V. Philips,October 14 & 15, Hack.lu 2005

[12] WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement By A.K.M. Nazmus Sakib, Shamim Ahmed, Samiur Rahman, Ishtiaque Mahmud & Md. Habibullah Belali Dhaka International University (DIU), Dhaka

[13] " Vulnerabilities of Wireless Security protocols (WEP and WPA2)" Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 2, April 2012

[14] "Security Improvement of WPA 2 (Wi-FiProtected Access 2)A.K.M. Nazmus Sakib CSE Department, Chittagong University of Engineering & Technology,Chittagong, BangladeshFariha Tasmin Jaigirdar Lecturer,Dept of Computer ScienceStamford University, Bangladesh Muntasim Munim Programmer Affiliation : Bangladesh Computer Society Armin Akter ,CSE Department, Chittagong University of Engineering & Technology, Chittagong, Bangladesh, A.K.M. Nazmus Sakib et al. / International Journal of Engineering Science and Technology (IJEST)

[15] "Overview of Wi-Fi Security What is left?" Philippe Teuwen,Security Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group ,N.V. Philips October 14 & 15 Hack.lu 2005

[16] Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) Paul Arana INFS 612 – Fall 200

www.takbook.com