تهیه و تنظیم :سعید عاقلي تازه شهري

نام پروژه: امنیت شبکه وایرلس

شماره تماس : ۰۹۱٤۳۸۸۰٦۹٦---۰۹۳٥۹۳٥۸۰۲۲

امنیـــت در شبـــــکه‌های بی‌سی‌ـــــم

بخش اول : مقدمه

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت.

شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌ای از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی است که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عملکرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل‌توجهی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد.

به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند.

منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول:
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 سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها 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 دهنده‌گان 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 :

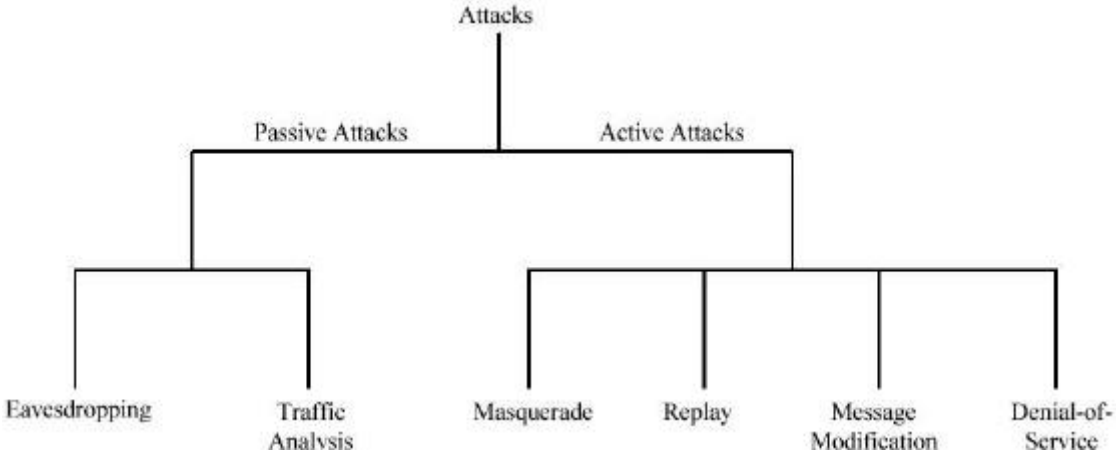
- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه ایی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه ا یی دست یابند.
- اطلاعات حیاتی ایی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می باشند، 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، به‌راحتی 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 حساس‌تری 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.

خطرها، حملات و ملزومات امنیتی (بخش اول)

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

تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازم.

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



-
- مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.
-
- حملات غیرفعال
- در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.
-
- - شنود
- در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.
-
- - آنالیز ترافیک
- در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.
-
- حملات فعال
- در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند :
-
- - تغییر هویت
- در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.
-
- - پاسخ های جعلی
- نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید

تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه -به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیامُ

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

- حمله های DoS) Denial-of-Service)

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

- **بخش دوم : شبکه های محلی بی‌سیم**

در این قسمت، به‌عنوان بخش دوم از بررسی امنیت در شبکه‌های بی‌سیم، به مرور کلی شبکه‌های محلی بی‌سیم می‌پردازم. اطلاع از ساختار و روش عملکرد این شبکه‌ها، حتی به صورت جزءیی، برای بررسی امنیتی لازم به‌نظر می‌رسد.

- **پی‌شی‌نه**

تکنولوژی و صنعت WLAN به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌های محلی بی‌سیم به کندی صورت می‌پذیرفت. با ارایه‌ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه‌های محلی امکان‌پذیر می‌ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی

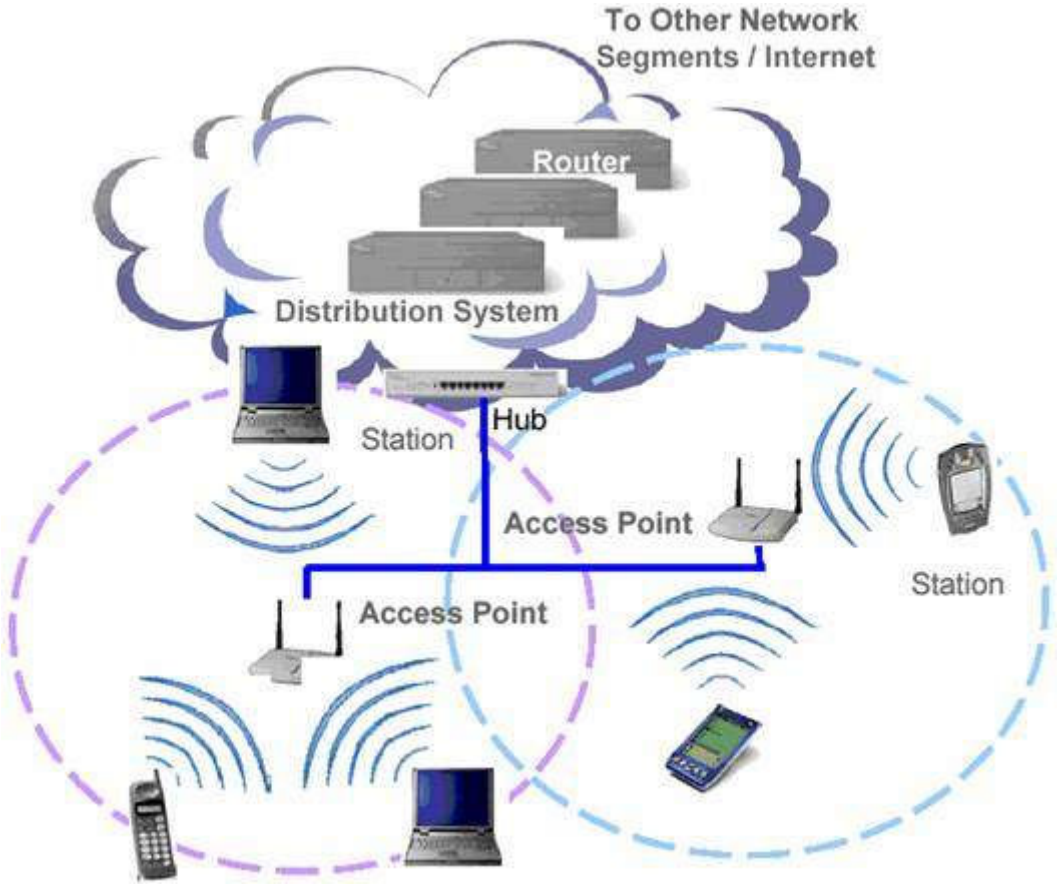
پروتکل‌ها و استانداردهای خانواده‌ی IEEE 802.11 است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می‌دهد

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

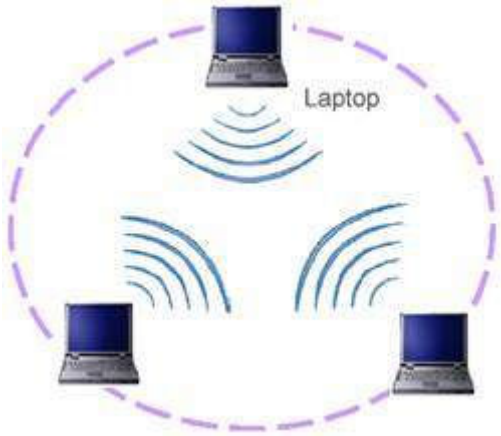
- اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می‌کند. با این وجود تعداد کانال‌های قابل استفاده در نوع b در مقایسه با نوع a، بیشتر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می‌کند. در حالت معمول، مقصود از WLAN استاندارد 802.11b است.
- استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به 802.11g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل 2.4GHz عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی‌شدن و معرفی آن نمی‌گذرد، بیش از یک‌سال است که آغاز شده و با توجه سازگاری آن با استاندارد 802.11b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.
- **معماری شبکه‌های محلی بی‌سیم**
- استاندارد 802.11b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه –همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود– و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).
- معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان

یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS(Basic Service Set) می‌نامند. مجموعه‌ی تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS(Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

-
- در سمت هریک از سخت‌افزارها که معمولاً مخدوم هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :
-



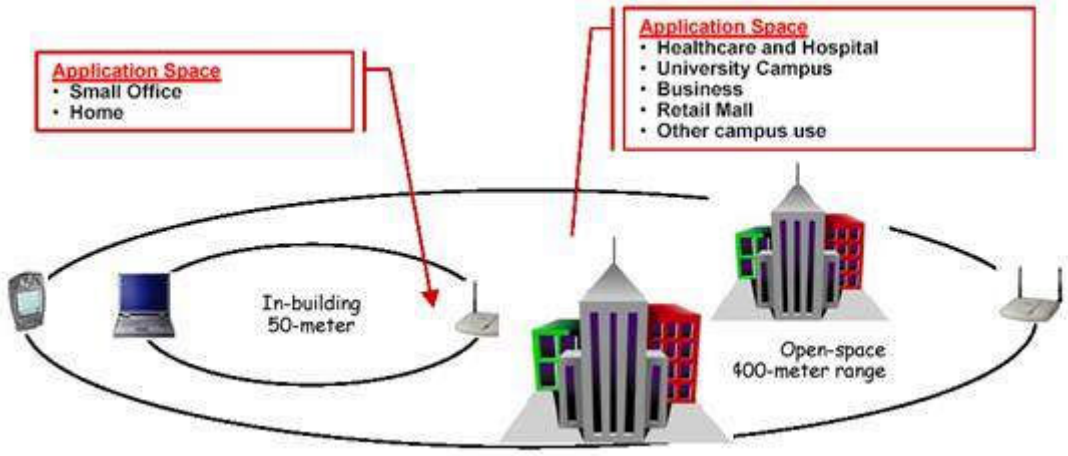
-
- همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یک نقطه‌ی مرکزی برای دسترسی وجود ندارد و سخت‌افزارهای همراه - مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایل - با ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خوانده می‌شوند. شکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد :
-



- شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

- **بخش سوم : عناصر فعال و سطح پوشش WLAN**
- عناصر فعال شبکه‌های محلی بی‌سیم
- در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد :
- ایستگاه بی سیم
- ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.
- کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.
- **نقطه ی دسترسی**
- نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سویچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

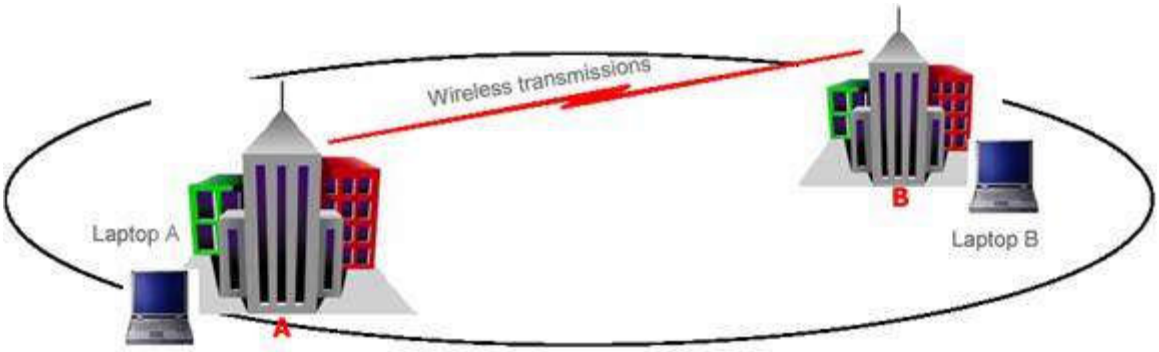
- برد و سطح پوشش
-
- شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بسته‌گی دارد که برخی از آن‌ها به شرح زیر هستند :
-
- – پهنای باند مورد استفاده
- – منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- – مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- – قدرت امواج
- – نوع و مدل آنتن
-
- شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرتمندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.
-
- با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عملکرد مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.
-
- شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :



-
-
- یکی از عملکردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عملکردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.
-
- اتصال میان نقاط دسترسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.
-
- نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و

این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد.

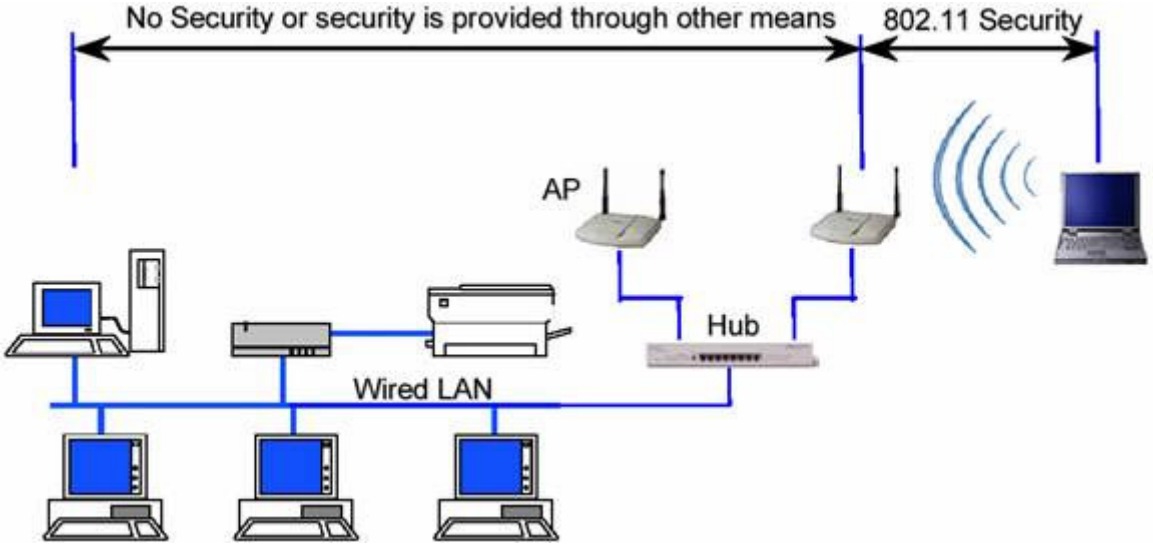
-
- شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می‌دهد :
-
-



-
-
- از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دسترسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

بخش چهارم : امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

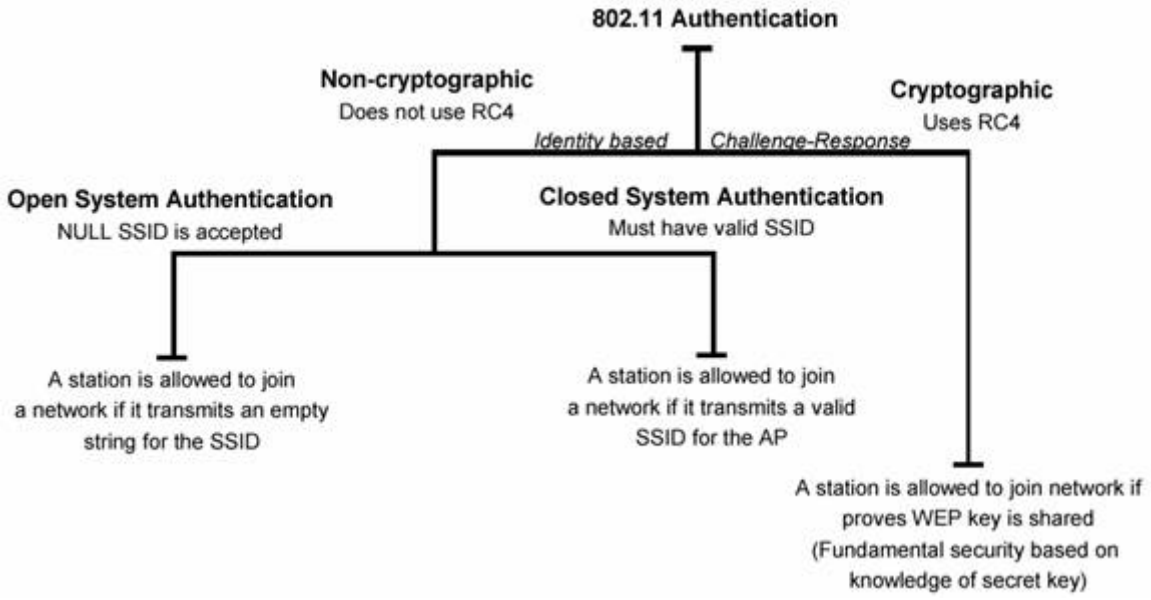
- پس از آن‌که در سه قسمت قبل به مقدمه‌یی در مورد شبکه‌های بی‌سیم محلی و عناصر آن‌ها پرداختیم، از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد.
- استاندارد 802.11 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 مخدوم‌ها 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 لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.
-



-
-
- شکل بالا محدوده‌ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می‌دهد.
-
- قابلیت‌ها و ابعاد امنیتی استاندارد 802.11
-
- در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های 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 مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های 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 ·
- 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 مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.
-
-
- Confidentiality ·
- محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

- Integrity .
- هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.
- نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing و Authorization در میان سرویس‌های ارایه شده توسط این پروتکل است.

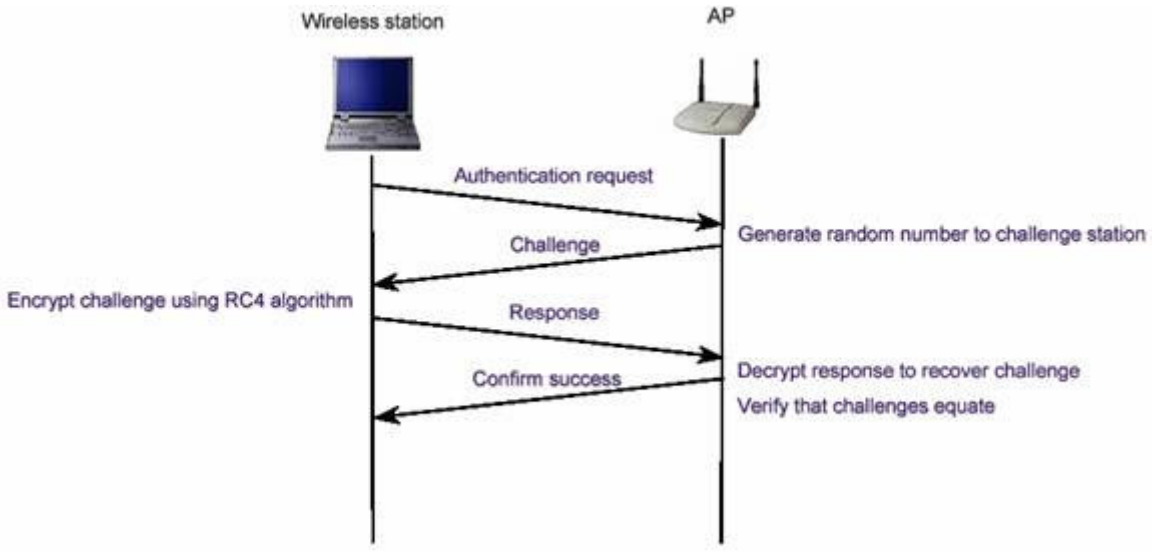
- **بخش پنجم : سرویس‌های امنیتی WEP - Authentication**
- در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد 802.11 است پرداخته شد و در ادامه سه سرویس اصلی این پروتکل را معرفی مي شود .
- در این قسمت به معرفی سرویس اول، یعنی Authentication، پرداخته مي شود .
- Authentication
- استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.
- شکل زیر شمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد :



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

- Authentication بدون رمزنگاری
- در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدوم متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می‌دهد.
-
- در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.
-
- در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.
-
- نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی است که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم - که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است - اطمینان از شانس پایین رخدادن حملات نیز خود تضمینی ندارد!

- Authentication با رمزنگاری RC4
- این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد :
-



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

- در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است :
- الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت مخدوم اطمینان حاصل می‌کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمزی است که نقطه‌ی دسترسی اصلی است.
-
- ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هریک از دو طرف را گمراه می‌کند.

بخش ششم : سرویس‌های امنیتی 802.11b – Privacy و Integrity

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

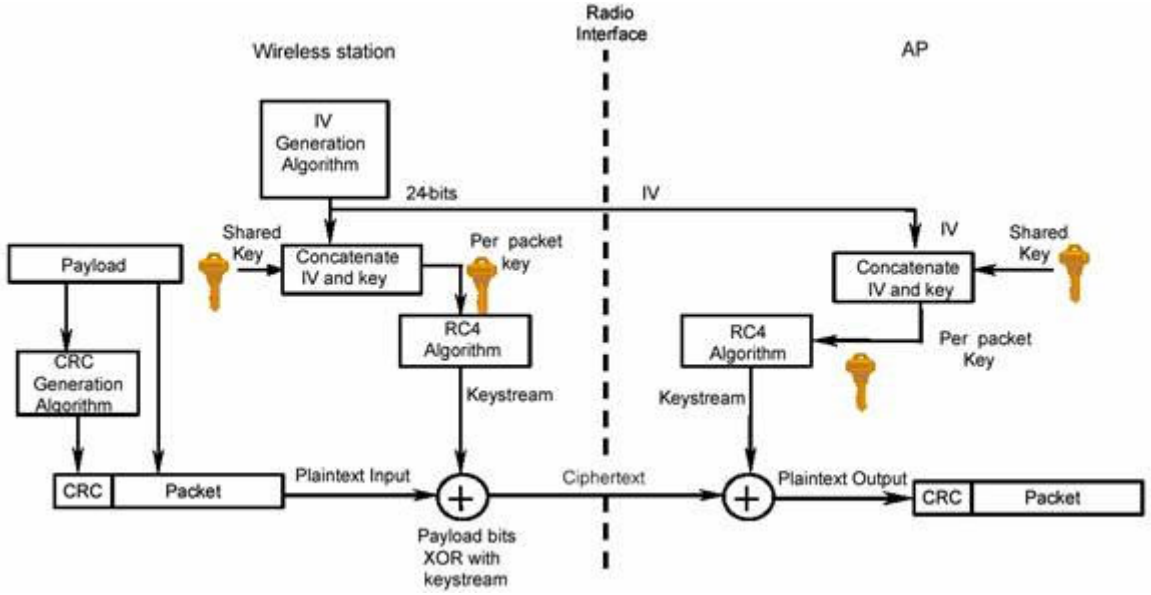
- Privacy
- این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه‌داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی‌که در صورت شنود اطلاعات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

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

- کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً

هرچه اندازه‌ی کلید بزرگتر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

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



- Integrity
- مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.
-
- در استاندارد 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC 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 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به‌صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگتر بیشتر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

بخش هفتم : ضعف‌های اولیه‌ی امنیتی WEP

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

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

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

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

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

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

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

- ۲. Initialization Vector (IV)
- این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.
- این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

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

- ۴. استفاده از CRC رمز نشده
- در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دسترسی بی‌سیم به‌سوی گیرنده ارسال می‌شود بر اساس یک CRC رمزنشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به‌راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دسترسی بماند که آیا بسته‌ی تأیید را صادر می کند یا خیر.

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

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 [illegible] WEP.**	The combination of revealing 24 key bits in the IV and a [illegible] 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

هفت مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱ (بخش اول)

- موفقیت حیرت انگیز ۸۰۲.۱۱ به علت توسعه «اترنت بی سیم» است. همچنانکه ۸۰۲.۱۱ به ترقی خود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است .در حالیکه همه مدیران شبکه باید درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد .

در این سلسله مقاله هفت مشکل از مهم ترین آسیب پذیری های امنیتی موجود درLAN 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 خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند 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 .

مسأله شماره ۱: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های Beacon با پارامتر های شبکه را ارسال کنند .البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های Beacon توسط هیچ 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 شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند .

راه حل شماره ۱: 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 ازVPN ها 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. ۸۰۲.۱ xانواع 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 برایLAN هاست 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 ۸۰۲.۱ xرا دنبال می کنند، ثابت کرده اند که برای استفاده درLAN های استفاده کننده از ۸۰۲.۱ xفوق العاده باارزش هستند .

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 ۸۰۲.۱ xرا 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، خصوصاً اگرLAN های 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 مانندVPN ها یا ۸۰۲.۱ xاستفاده نمی کنند، علائم هشداردهنده را ثبت کنند

- **هفت مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱ :بخش دوم**
- **مسأله شماره ۲: 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 .

راه حل شماره۲ : 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 ۸۰۲.۱۱ aبه عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های ۸۰۲.۱۱ aرا بوجود آورد. خوشبختانه، ۸۰۲.۱۱ aاز 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 استاندارد ۸۰۲.۱۱ aو ۸۰۲.۱۱ bرا بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند .چیپ ست های دوباندی ۸۰۲.۱۱ a/bو 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 چارچوپ پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا ۸۰۲.۱۱ gادامه یابد، تا جایی که سازندگان آنالایزرها کارت های ۸۰۲.۱۱ a/b/gرا مورد پذیرش قرار دهند .

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 802.11 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 ۸۰۲.۱۱ bرا انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی ۸۰۲.۱۱ aرا 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 ۸۰۲.۱۱ bبه کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا

۱۱ از ۸۰۲.۱۱ bرا می دهد. کانال های ۱۲ تا ۱۴ 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.

هفت مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱ :بخش سوم

- **مسأله شماره ۳: 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 نکرده اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنند گان محصولات استفاده می شوند. بدون WEP دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسی باز می تواند بروز کند: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی کنند، و نیز ممکن است تنها توسط یک اسپم ساز اتصال شما بهISP تان لغو شود .

راه حل شماره۳ : طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجاز به شبکه است. تأیید هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صدور اجازه است، زیرا امتیازات دسترسی برپایه هویت کاربر قرار دارند. روش های VPN که برای حفاظت از انتقال در لینک رادیویی به کارگرفته می شوند، تأیید هویت محکمی را ارائه می کنند. تخمین مخاطرات انجام شده توسط سازمان ها نشان می دهد که دسترسی به 802.1xباید توسط روش های تأیید هویت برپایه رمزنگاری تضمین شود. 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 تبعیت از سیاست های تایید هویت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در این راه حل نیز نظارت های منظمی بر تجهیزات شبکه بی سیم باید انجام شود تا استفاده از مکانیسم های تأیید هویت و پیکربندی مناسب ابزارهای شبکه تضمین

شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو باند فرکانسی ۸۰۲.۱۱) bباند (2.4 GHz ISM و ۸۰۲.۱۱ (5 GHz U-NII) aتشخیص دهد و پارامترهای عملیاتی مرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسیور دستی می 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 .

مسأله شماره ۴ : محدودیت های سرویس و کارایی

LANهای بی سیم ظرفیت های ارسال محدودی دارند. شبکه های ۸۰۲.۱۱ bسرعت انتقالی برابر با ۱۱ Mbps و شبکه های برپایه تکنولوژی جدید ۸۰۲.۱۱ a نرخ انتقال اطلاعاتی تا ۵۴ Mbps دارند .البته ماحصل مؤثر واقعی، به دلیل بالاسری لایهMAC ، تقریباً تا نیمی از ظرفیت اسمی می رسد. نقاط دسترسی کنونی این ظرفیت محدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت می کنند. تصور اینکه چگونه برنامه های محلی احتمالاً چنین ظرفیت محدودی را اشغال می کنند یا چگونه یک نفوذگر ممکن است یک حمله انکار سرویس (DoS) روی این منابع محدود طرح ریزی کند، سخت نیست.

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 .

راه حل شماره۴ : 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 .

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.

هفت مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱ – بخش چهارم

- **مسأله شماره ۵: 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 ARP (Address Resolution Protocol) استفاده کنند. در سطحی بسیار ساده تر، نفوذگران می توانند آدرس های MAC (Medium Access Control) 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 ۸۰۲.۱ **X** است که در ژوئن ۲۰۰۱ تصویب شده است. ۸۰۲.۱ **X** می 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 SSID (Service Set Identifier) که معمولاً network name نیز نامیده می شود، منتشر می کند، به عنوان بخشی از شبکه مجاز به نظر خواهد رسید. به 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 ۸۰۲.۱ xوجود 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 ۸۰۲.۱۱ MAC تصدیق هویت در هر فریم را به عنوان بخشی از ۸۰۲.۱۱ اپذیرد .

راه حل شماره۵ : پذیرش پروتکل های قوی و استفاده از آنها

تا زمان تصویب ۸۰۲.۱۱ اجعل 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 ۸۰۲.۱ xداشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق ۸۰۲.۱x، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت ۸۰۲.۱ xارائه 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.

هفت مشکل امنیتی مهم شبکه های بی سیم ۸۰۲.۱۱ – بخش آخر
مسأله شماره ۶: تحلیل ترافیک و استراق سمع

802.11هیچ 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 (Wired WEP) 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 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.

راه حل شماره۶ : 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 مانندSSH ، SSLو 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 ازWEP ، 802.1xو 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.

علاوه بر استفاده از پروتکل های VPN قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی کاربر با استفاده از ۸۰۲.۱ Xداشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق ۸۰۲.۱X، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت ۸۰۲.۱ Xارائه 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.

مسأله شماره ۷: 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.

راه حل شماره۷ : 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.

نتیجه گیری

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