

" امنیت در شبکه های بی سیم "

مقدمه :

از آن جا که شبکه های بی سیم، در دنیای کنونی هر چه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. 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، بنا داریم در این بخش با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه ها با تأکید بر ابعاد امنیتی آن ها، به روش های پیکربندی صحیح که احتمال رخ داد حملات را کاهش می دهند، بپردازیم.

📌 شبکه های بی سیم، کاربردها، مزایا و ابعاد :

تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط امواج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان می دهد تا بدون استفاده از بستری های فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه های بی سیم بازه ی وسیعی از کاربردها، از ساختارهای پیچیده یی چون شبکه های بی سیم سلولی - که اغلب برای تلفن های همراه استفاده می شود- و شبکه های محلی بی سیم (WLAN – Wireless LAN) گرفته تا انواع ساده یی چون هدفون های بی سیم، را شامل می شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می کنند، مانند صفحه کلیدها، ماوس ها و برخی از گوشی های همراه، در این دسته بندی جای می گیرند. طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و همچنین امکان ایجاد تغییر در ساختار مجازی آن هاست. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردند : WLAN، WWAN و WPAN.

شبکه های WPAN از سوی دیگر در دسته ی شبکه های Ad Hoc نیز قرار می گیرند. در شبکه های Ad hoc، یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می شود. مثالی از این نوع شبکه ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرار گرفتن 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. به عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستا است درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده‌کنندگان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه‌حل‌های 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. به عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به حساب 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 معرفی کرده 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 حقایق مشترک صادق است:

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌ی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان‌گونه که ذکر شد مخاطرات ویژه‌ی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌ی 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 شبکه های بی سیم، می توانند به شبکه ی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می تواند رفتار یک کاربر را پایش کند. از این طریق می توان به اطلاعات حساس دیگری نیز دست یافت.
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه ی استفاده از شبکه ی بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگر می تواند از نقاط مشترک میان یک شبکه ی بی سیم در یک سازمان و شبکه ی سیمی آن (که در اغلب موارد شبکه ی اصلی و حساس تری محسوب می گردد) استفاده کرده و با نفوذ به شبکه ی بی سیم عملاً راهی برای دستیابی به منابع شبکه ی سیمی نیز بیابد.
- در سطحی دیگر، با نفوذ به عناصر کنترل کننده ی یک شبکه ی بی سیم، امکان ایجاد اختلال در عملکرد شبکه نیز وجود دارد.

با مقدمه ی ذکر شده، در قسمت های آتی می توانیم به ویژه گی های این شبکه های، با تفکیک تکنولوژی های مرسوم، از بعد امنیتی بپردازیم و چگونه گی پیکربندی صحیح یک شبکه ی بی سیم را، برای بالابردن امنیت آن، بررسی کنیم.

شبکه های محلی بی سیم:

در این قسمت، به عنوان بخش دوم از بررسی امنیت در شبکه های بی سیم، به مرور کلی شبکه های محلی بی سیم می پردازیم. اطلاع از ساختار و روش عمل کرد این شبکه ها، حتی به صورت جزئی، برای بررسی امنیتی لازم به نظر می رسد.

پیشینه

تکنولوژی و صنعت WLAN به اوایل دهه ی ۸۰ میلادی باز می گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه های محلی بی سیم به کندی صورت می پذیرفت. با ارایه ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه های محلی امکان پذیر می ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل ها و استانداردهای خانواده ی IEEE 802.11 است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می دهد

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 شبکه ی محلی بی سیم تجاری توسط Motorola پیاده سازی شد. این شبکه، به عنوان یک نمونه از این شبکه ها، هزینه ی بالا و پهنای باندی پایین را تحمیل می کرد که ایداً مقرون به صرفه نبود. از همان زمان به بعد، در اوایل دهه ی ۹۰ میلادی، پروژه ی 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 پایه ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می کند. در حالی که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می کند. با این وجود تعداد کانال های قابل استفاده در نوع b در مقایسه با نوع a، بیش تر است. تعداد این کانال ها، با توجه به کشور مورد نظر، تفاوت می کند. در حالت معمول، مقصود از WLAN استاندارد 802.11b است.

استاندارد دیگری نیز به تازگی توسط IEEE معرفی شده است که به **802.11g** شناخته می شود. این استاندارد بر اساس فرکانس حامل **2.4GHz** عمل می کند ولی با استفاده از روش های نوینی می تواند پهنای باند قابل استفاده را تا **54Mbps** بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی شدن و معرفی آن نمی گذرد، بیش از یک سال است که آغاز شده و با توجه سازگاری آن با استاندارد **802.11b**، استفاده از آن در شبکه های بی سیم آرام آرام در حال گسترش است.

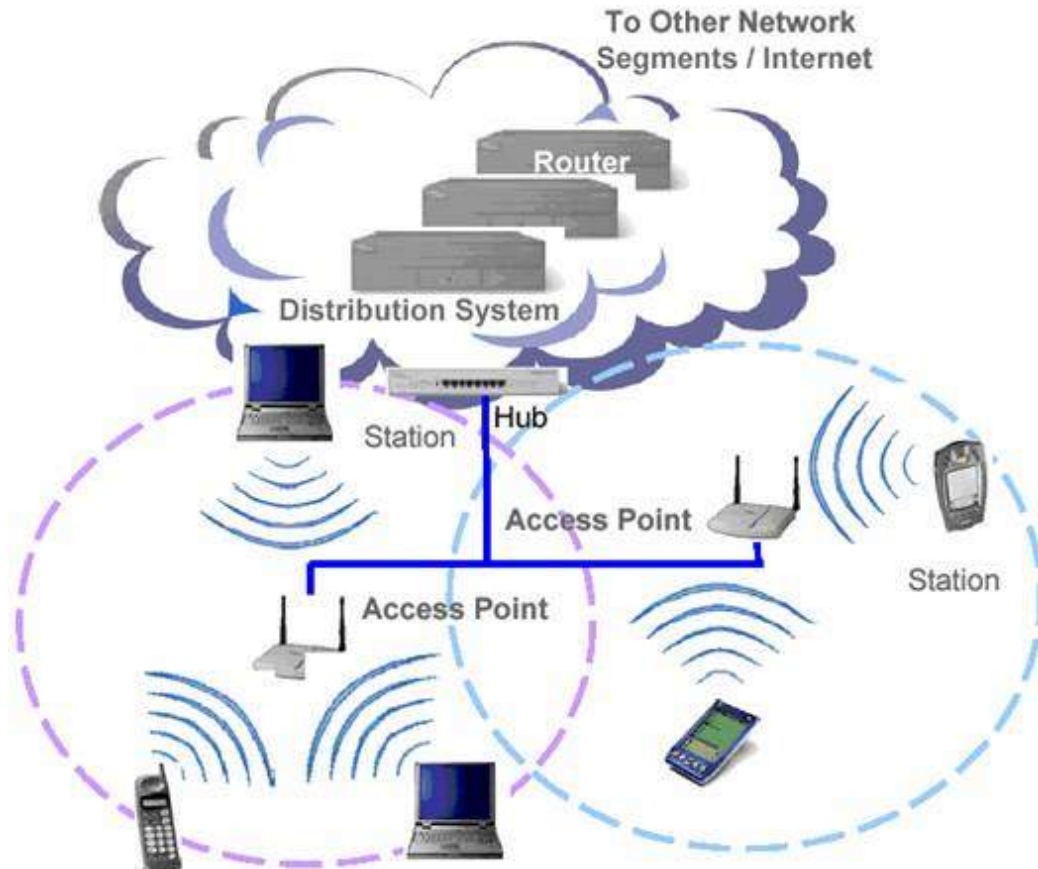
معماری شبکه های محلی بی سیم

استاندارد **802.11b** به تجهیزات اجازه می دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارتند از برقراری ارتباط به صورت نقطه به نقطه - همان گونه در شبکه های **Ad hoc** به کار می رود - و اتصال به شبکه از طریق نقاط تماس یا دسترسی (**AP=Access Point**).

معماری معمول در شبکه های محلی بی سیم بر مبنای استفاده از **AP** است. با نصب یک **AP**، عملاً مرزهای یک سلول مشخص می شود و با روش هایی می توان یک سخت افزار مجهز به امکان ارتباط بر اساس استاندارد **802.11b** را میان سلول های مختلف حرکت داد. گستره ای که یک **AP** پوشش می دهد را **BSS(Basic Service Set)** می نامند. مجموعه ای تمامی سلول های یک ساختار کلی شبکه، که ترکیبی از **BSS** های شبکه است، را **ESS(Extended Service Set)** می نامند. با استفاده از **ESS** می توان گستره ای وسیع تری را تحت پوشش شبکه ای محلی بی سیم در آورد.

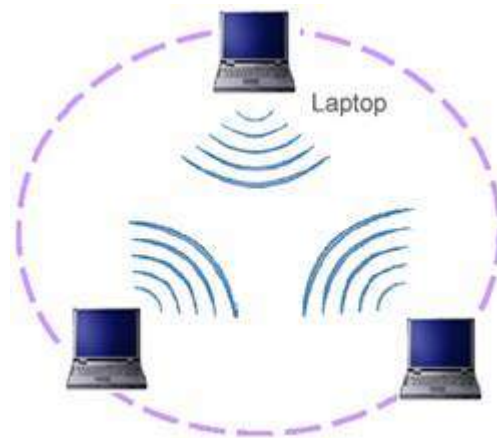
در سمت هریک از سخت افزارها که معمولاً مخدوم هستند، کارت شبکه ایی مجهز به یک مودم بی سیم قرار دارد که با **AP** ارتباط را برقرار می کند. **AP** علاوه بر ارتباط با چند کارت شبکه ای بی سیم، به بستر پرسرعت تر شبکه ای سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم های مجهز به کارت شبکه ای بی سیم و شبکه ای اصلی برقرار می شود.

شکل زیر نمایی از این ساختار را نشان می دهد :



همان گونه که گفته شد، اغلب شبکه های محلی بی سیم بر اساس ساختار فوق، که به نوع **Infrastructure** نیز موسوم است، پیاده سازی می شوند. با این وجود نوع دیگری از شبکه های محلی بی سیم نیز وجود دارند که از همان منطق نقطه به نقطه استفاده می کنند. در این شبکه ها که عموماً **Ad hoc** نامیده می شوند یک نقطه ی مرکزی برای دسترسی وجود ندارد و سخت افزارهای همراه - مانند کامپیوترهای کیفی و جیبی یا گوشی های موبایل - با ورود به محدوده ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می گردند. این شبکه ها به بستر شبکه ی سیمی متصل نیستند و به همین منظور **IBSS (Independent Basic Service Set)** نیز خواند می شوند.

شکل زیر شمایی ساده از یک شبکه ی Ad hoc را نشان می دهد :



شبکه های Ad hoc از سویی مشابه شبکه های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه یی به عنوان سرورس دهنده وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می توانند پرونده های مورد نظر خود را با دیگر گره ها به اشتراک بگذارند.

در قسمت بعد، به دسته بندی اجزای فعال یک شبکه ی محلی بی سیم پرداخته و شعاع پوشش این دسته از شبکه ها را مورد بررسی قرار خواهیم داد.

عناصر فعال و سطح پوشش WLAN

در شبکه های محلی بی سیم معمولاً دو نوع عنصر فعال وجود دارد :

✓ ایستگاه بی سیم

ایستگاه یا سرورس گیرنده بی سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه ی بی سیم به شبکه ی محلی متصل می شود. این ایستگاه می تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویس گر بارکد نیز باشد. در برخی از کاربردها برای این که استفاده از سیم در پایانه های رایانه یی برای طراح و مجری دردسرساز است، برای این پایانه ها که معمولاً در داخل کیوسک هایی به همین منظور تعبیه می شود، از امکان اتصال بی سیم به شبکه ی محلی استفاده می کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه ی بی سیم نیست.

کارت های شبکه ی بی سیم عموماً برای استفاده در چاک های PCMCIA است. در صورت نیاز به استفاده از این کارت ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت ها را بر روی چاک های گسترش PCI نصب می کنند.

✓ نقطه ی دسترسی :

نقاط دسترسی در شبکه های بی سیم، همان گونه که در قسمت های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه های بی سیم را بازی کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم ها و ایستگاه های بی سیم به شبکه ی سیمی اصلی متصل می گردد.

✚ برد و سطح پوشش

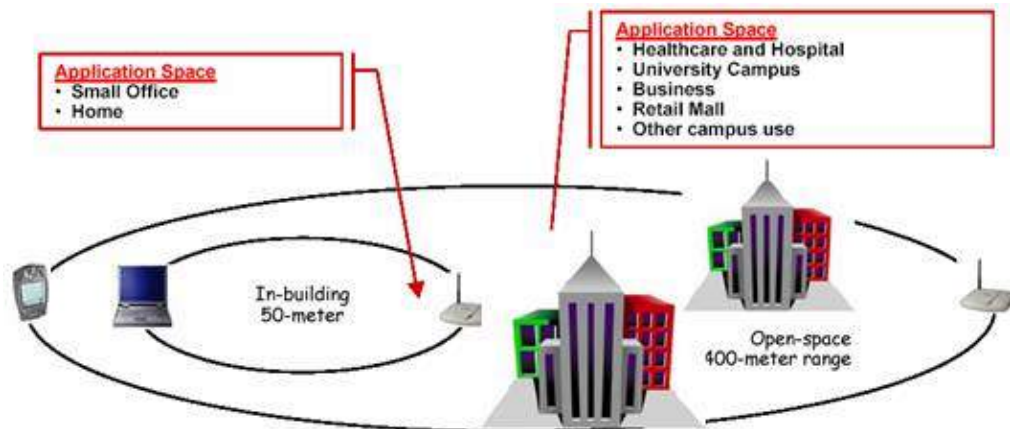
شعاع پوشش شبکه ی بی سیم بر اساس استاندارد 802.11b به فاکتورهای بسیاری بسته گی دارد که برخی از آن ها به شرح زیر هستند :

- ✓ پهنای باند مورد استفاده
- ✓ منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها
- ✓ مشخصات فضای قرارگیری و نصب تجهیزات شبکه ی بی سیم
- ✓ قدرت امواج
- ✓ نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹ متر (برای فضاهای بسته ی داخلی) و ۴۸۵ متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده ها و فرستنده های نسبتاً قدرتمندی که مورد استفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونه های عملی آن فراوان اند.

با این وجود شعاع کلی بی که برای استفاده از این پروتکل (802.11b) ذکر می شود چیزی میان ۵۰ تا ۱۰۰ متر است. این شعاع عمل کرد مقداری ست که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و می تواند مورد استناد قرار گیرد.

شکل زیر مقایسه‌ی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد:

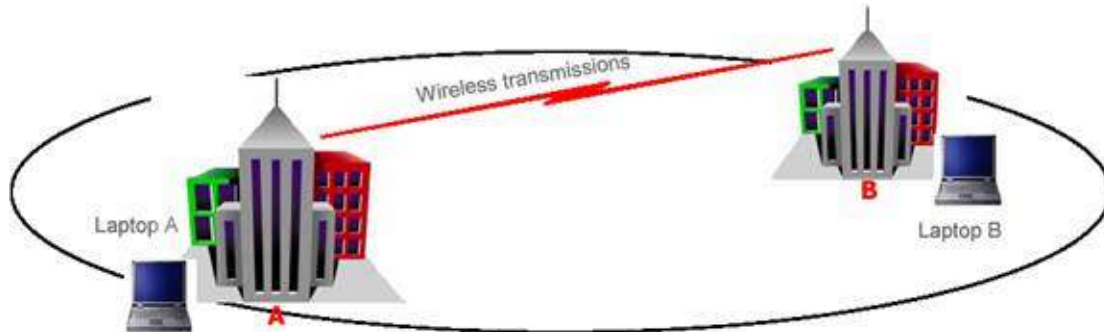


یکی از عمل‌کردهای نقاط دسترسی به عنوان سویچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به عبارت دیگر با استفاده از چند سویچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به دست آورد.

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 به صورت همزمان صورت گیرد.

نقاط دسترسی بی‌ی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌ی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به دست 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 بی سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی سیم، می‌توان از چند نقطه‌ی دسترسی بی سیم به صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هر یک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

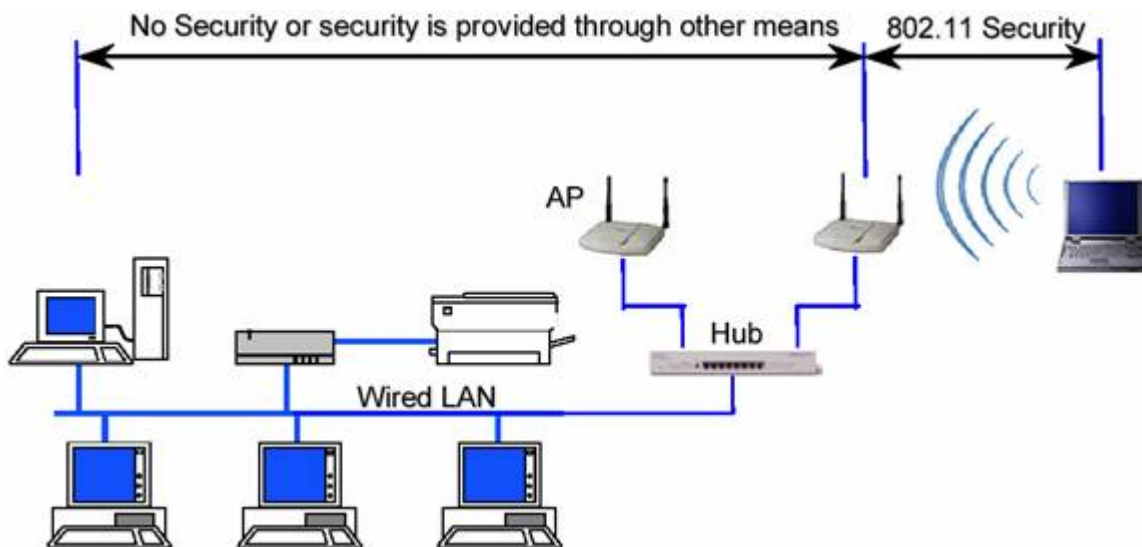
در قسمت بعد به مزایای معمول استفاده از شبکه‌های محلی بی سیم و ذکر مقدماتی در مورد روش‌های امن سازی این شبکه‌ها می‌پردازیم.

امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن که در سه قسمت قبل به مقدمه‌یی در مورد شبکه‌های بی سیم محلی و عناصر آن‌ها پرداختیم، از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی سیم 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 بی سیم 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 بی سیم 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 بی سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که

استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل بالا محدوده ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می دهد.

قابلیت ها و ابعاد امنیتی استاندارد 802.11:

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم بر اساس استاندارد 802.11 فراهم می کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت این است که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هرچند جزئی میان امنیت در شبکه های سیمی و بی سیمی است که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

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

Authentication ✓

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

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 شبکه ی محلی بی سیم است.

Integrity ✓

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

نکته ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس های معمول Auditing و Authorization در میان سرویس های ارایه شده توسط این پروتکل است.

در قسمت های بعدی از بررسی امنیت در شبکه های محلی بی سیم به بررسی هر یک از این سه سرویس می پردازیم.

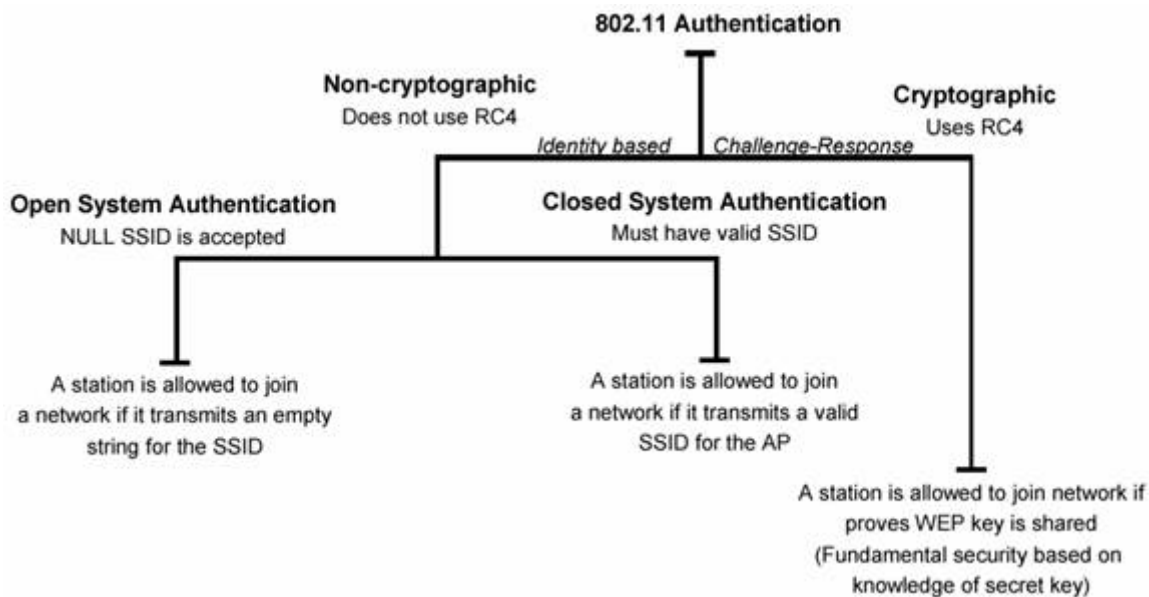
🚩 سرویس های امنیتی WEP - Authentication

در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن سازی ارتباطات در شبکه های بی سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم. در این قسمت به معرفی سرویس اول، یعنی Authentication، می پردازیم.

Authentication ✓

استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه ی بی سیم را به نقاط دسترسی ارسال می کنند، دارد که یک روش بر مبنای رمزنگاری ست و دیگری از رمزنگاری استفاده نمی کند.

شکل زیر شمایی از فرایند Authentication را در این شبکه ها نشان می دهد :



همان گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری بی استفاده نمی کند.

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 می دهد.

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

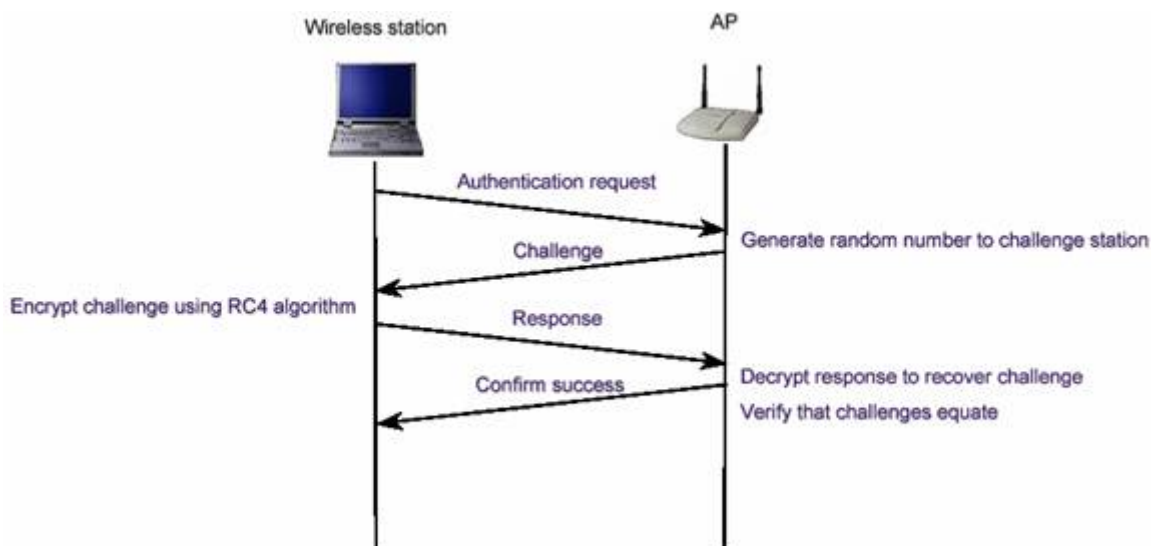
در روش دوم از این نوع، باز هم یک SSID به نقطه‌ی دسترسی ارسال می گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌ی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی است که این روش در اختیار ما می گذارد. این دو روش عملاً روش امنی از احراز هویت را ارائه نمی دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست کننده هستند. با این وصف از آنجایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق

بسیاری، حتی توسط نفوذگران کم تجربه 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 رخ دادن 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 آن را 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 دسترسی است 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 رمزپسند است نقطه‌ی دسترسی اصلی است.

ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سؤال 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 به‌گونه‌ی هریک از دو طرف را گمراه می‌کند. در قسمت بعد به سرویس‌های دیگر پروتکل **WEP** می‌پردازیم.

🚩 سرویس‌های امنیتی **802.11b** Privacy و Integrity

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

✓ Privacy

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

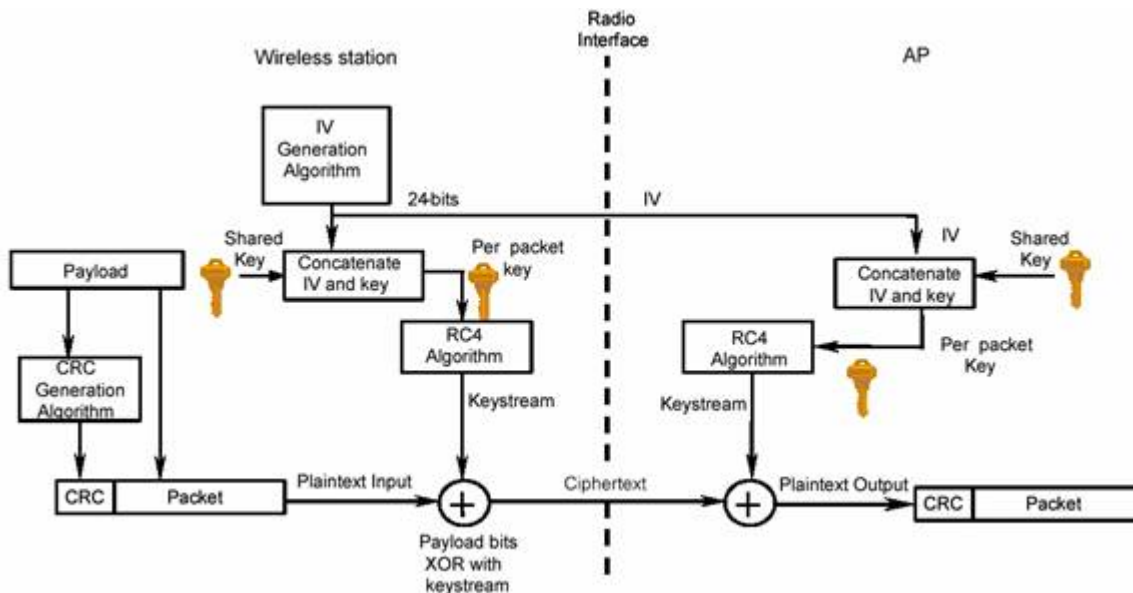
در استاندارد **802.11b**، از تکنیک‌های رمزنگاری **WEP** استفاده می‌گردد که برپایه‌ی **RC4** است. **RC4** یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به بیان دیگر داده‌های تمامی لایه‌های 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 به اختصار **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 تعداد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌ی بالاست که قدرت پردازش سیستم‌های رایانه‌ی 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 نکته‌ی که اخیراً بر اساس یک سری آزمایشات به دست آمده است، این است 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 رمز شدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، **CRC** داده‌های رمزگشایی شده مجدداً محاسبه شده و با **CRC** نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو **CRC** به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط **RC4**، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد **802.11b** هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضله‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهولت انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییر ندادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی‌ها نتیجه‌ی جز درصد نسبتاً بالایی

از حملات موفق به شبکه های بی سیم ندارد. این مشکل از شبکه های بزرگ تر بیش تر خود را نشان می دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل انگاری هایی، زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گه گاه خطاهایی در گوشه و کنار این شبکه ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود.

در قسمت بعد به مشکلات و ضعف هایی که سرویس های امنیتی در استاندارد 802.11b دارند می پردازیم.

✚ ضعف های اولیه ی امنیتی WEP :

در قسمت های قبل به سرویس های امنیتی استاندارد 802.11 پرداختیم. در ضمن ذکر هریک از سرویس ها، سعی کردیم به ضعف های هریک اشاره یی داشته باشیم. در این قسمت به بررسی ضعف های تکنیک های امنیتی پایه ی استفاده شده در این استاندارد می پردازیم.

همان گونه که گفته شد، عملاً پایه ی 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 می شود، هرچند که برخی از تولیدکننده گان نگارش های خاصی از WEP را با کلیدهایی با تعداد بیت های بیش تر پیاده سازی کرده اند.

نکته یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه ی کلیدهاست. با وجود آن که با بالارفتن اندازه ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می رود، ولی از آن جاکه این کلیدها توسط کاربران و بر اساس یک کلمه ی عبور تعیین می شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان طور که در قسمت های پیشین نیز ذکر شد، دست یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است. حاصل بررسی های انجام شده فهرستی از ضعف های اولیه ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP:

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دسترس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه های کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های 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 آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس IV تولید می شود، محدوده IV عملاً نشان دهنده احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می توان به کلیدهای مشابه دست یافت. این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ای استفاده شده مطمئن نباشیم. بسیاری از کارت های شبکه از IV های ثابت استفاده می کنند و بسیاری از کارت های شبکه ای یک تولید کننده واحد IV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه ای شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی ست نفوذگر در مدت زمانی معین به ثبت داده های رمز شده ای شبکه بپردازد و IV های بسته های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IV های استفاده شده در یک شبکه ای شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم:

از آن جایی که IV در تمامی بسته های تکرار می شود و بر اساس آن کلید تولید می شود، نفوذگر می تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IV ها و بسته های رمز شده 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 می گردد.

۴. استفاده از CRC رمز نشده :

در پروتکل WEP، کد CRC رمز نمی شود. لذا بسته های تأییدی که از سوی نقاط دسترسی بی سیم به سوی گیرنده ارسال می شود بر اساس یک CRC رمز نشده ارسال می گردد و تنها در صورتی که نقطه ای دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به راحتی عوض کند و منتظر عکس العمل نقطه ای دسترسی بماند که آیا بسته ای تأیید را صادر می کند یا خیر.

ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هستند. نکته ای که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می گردد و بقیه ای مشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول زیر ضعف‌های امنیتی پروتکل WEP را به اختصار جمع‌بندی کرده است :

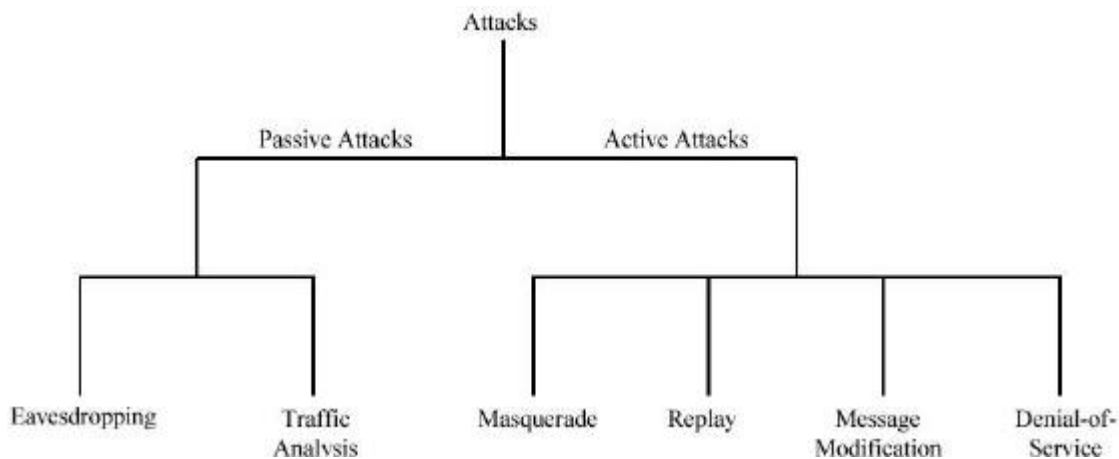
Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a compromise 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.

در قسمت‌های آتی به بررسی خطرهای ناشی از این ضعف‌ها و نیازهای امنیتی در شبکه‌های بی‌سیم می‌پردازیم.

✚ خطرها، حملات و ملزومات امنیتی :

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

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



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

✚ حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای 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 می‌آید، تغییر می‌دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می‌کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم‌بندی می‌گردند:

✓ تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می‌کند. این روش شامل تغییر هویت اصلی یکی از طرف‌های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می‌گردد.

✓ پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته‌هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می‌کند را پایش می‌کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می‌گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می‌گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می‌کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می‌گردند به معنای پرچمی برای شناسایی گیرنده محسوب می‌گردند. 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، می‌تواند 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 می‌گردد.

✓ تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه‌های متنوعی از ترافیک بر روی شبکه رفت و آمد می‌کنند و هریک از این ترافیک ها و پروتکل‌ها از شیوه‌ی برای مدیریت جنبه های امنیتی خود استفاده می‌کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می‌تواند 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 نمی‌توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می‌کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می‌تواند با اعمال تغییرات خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دسترسی - که می‌تواند یک کاربر عادی باشد - فراهم کند.

✓ حمله های (Denial-Of-Service) DOS

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می‌شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می‌کند. ساده ترین نمونه سعی در از کارانداختن سرویس دهنده های نرم افزاری و سخت افزاری است. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه یی است که مشکلاتی برای نفوذگر برای دست رسی به اطلاعات

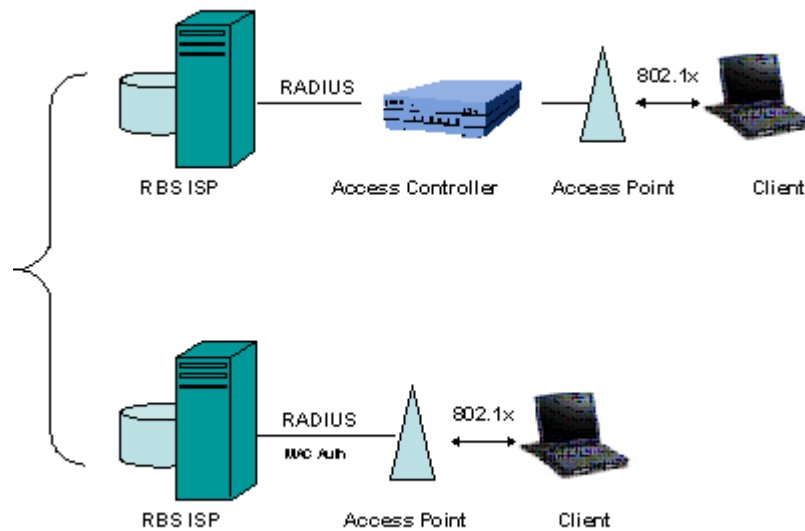
فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می‌کند. در برخی از حالات، در پی حمله‌ی انجام‌شده، سرویس مورد نظر به طور کامل قطع نمی‌گردد و تنها کارایی آن مختل می‌گردد. در این حالت نفوذگر می‌تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق/به همان سرویس نیز اقدام کند.

تمامی ریسک‌هایی که در شبکه‌های محلی، خصوصاً انواع بی‌سیم، وجود دارد ناشی از یکی از خطرات فوق است. در قسمت بعدی به دسته بندی و شرح این ریسک‌ها و پیامدهای آن‌ها می‌پردازیم.

هفت مشکل امنیتی مهم شبکه‌های بی‌سیم 802.11: بخش اول

موفقیت حیرت‌انگیز 802.11 به علت توسعه «اترنت بی‌سیم» است. همچنانکه 802.11 به ترقی خود ادامه می‌دهد، تفاوت‌هایش با اترنت بیشتر مشخص می‌شود. بیشتر این تفاوت‌ها به دلیل نا‌آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه‌ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می‌شوند. آنالایزهای (تحلیل‌کننده) شبکه‌های بی‌سیم برای مدت‌ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده‌اند. بسیاری از آنالایزها بعضی کارکردهای امنیتی را نیز اضافه کرده‌اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می‌دهد.

در این سلسله مقاله هفت مشکل از مهم‌ترین آسیب‌پذیری‌های امنیتی موجود در LAN‌های بی‌سیم، راه‌حل آنها و در نهایت چگونگی ساخت یک شبکه بی‌سیم امن مورد بحث قرار می‌گیرد. بسیاری از پرسش‌ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می‌توانند استفاده کنند. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می‌توانند برای تشخیص بسیاری از نگرانی‌های امنیتی که استفاده از شبکه بی‌سیم را کند می‌کنند، استفاده شوند. این سلسله مقاله هریک از این «هفت مسأله امنیتی» را بررسی می‌کند و توضیح می‌دهد که چگونه و چرا آنالایزر بی‌سیم، یک ابزار حیاتی برای تضمین امنیت شبکه‌های بی‌سیم است.



مسئله شماره ۱: دسترسی آسان

LAN‌های بی‌سیم به آسانی پیدا می‌شوند. برای فعال کردن کلاینت‌ها در هنگام یافتن آنها، شبکه‌ها باید فریم‌های Beacon با پارامترهای 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. فریم‌های Beacon توسط هیچ تابع اختصاصی پردازش نمی‌شوند و این به این معنی است که شبکه 802.11 شما و پارامترهایش برای هر شخصی با یک کارت 802.11 قابل استفاده است. نفوذگران با آنتن‌های قوی می‌توانند شبکه‌ها را در مسیرها یا ساختمان‌های 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 آسیب‌پذیری مترادف نیست. شبکه‌های بی‌سیم برای ایجاد امکان اتصال مناسب طراحی شده‌اند، اما می‌توانند با اتخاذ سیاست‌های امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی‌سیم

می‌تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی‌دهد. به هر حال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می‌تواند 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 VPN 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 بر پایه استاندارد IEEE 802.1x هستند. 802.1x انواع فریم‌های جدید برای تأیید هویت کاربر را تعریف می‌کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می‌گیرد. آنالیزهای باسیم سنتی می‌توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت 802.11 شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می‌کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می‌کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت 802.1x را دنبال می‌کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چپش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می‌دهند و می‌توانند چندین مسأله معمول امنیت 802.1x را تشخیص دهند. تعدادی از حملات روی شبکه های باسیم در سال‌های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه‌ها نشان می‌دهند. آنالیزهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می‌کنند و به این ترتیب مدیران شبکه می‌توانند 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 بی‌سیم بدون نظارت مهندسان امنیتی به کار گرفته شده باشند. موتورهای آنالیز خبره می‌توانند زمانی را که پیکربندی‌های پیش فرض کارخانه مورد استفاده قرار می‌گیرند، شناسایی کنند و به این ترتیب می‌توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالیزها همچنین می‌توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی‌کنند، علائم هشدار دهنده را ثبت کنند.

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 می‌توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می‌تواند 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 می‌شوند و لذا دپارتمان ها ممکن

است بتوانند LAN بی‌سیمشان 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 می‌کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LAN های بی‌سیم 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 بیکربندی پیش فرض نداشته اند و با همان بیکربندی راه اندازی شده اند.



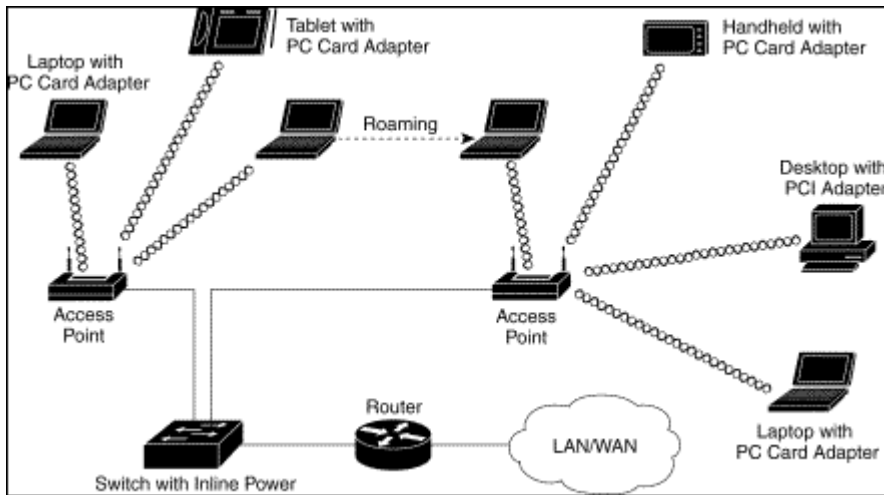
راه حل شماره ۲: رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی‌ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه‌های 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 استفاده‌های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفاده‌های 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 802.11 در سال های اخیر ظهور 802.11a به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های 802.11a را بوجود آورد. خوشبختانه، 802.11a از همان MAC پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجع به 802.11 و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد 802.11a و 802.11b را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست های دوباندی 802.11a/b و کارت های ساخته شده با آنها به آنالیزرها 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 **802.11g** ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های **802.11a/b/g** را مورد پذیرش قرار دهند.



بسیاری از ابزارها می‌توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک‌های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می‌توانند 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 پوشش کنند. حتی اگر شما استفاده از **802.11b** را انتخاب کرده اید، آنالایز استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی **802.11a** را نیز پوشش کند تا در طول یک بررسی کامل نیازی به جایگزین‌های سخت‌افزاری و نرم‌افزاری نباشد.

بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال‌های **802.11b** به‌کار بگیرند که برای ارسال استفاده نمی‌شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال‌های ۱ تا ۱۱ از **802.11b** را می‌دهد. کانال‌های ۱۲ تا ۱۴ جزء مشخصات آن تعریف شده اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هر حال، بعضی کاربران ممکن است از نقطه دسترسی کانال‌های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال‌های مطابق با FCC از کانال‌های 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 نمایندگی‌های مجاز برحذر باشند. آنالایزهای غیرفعال (**Passive Analyzers**) ابزار ارزشمندی هستند زیرا استفاده های غیرمجاز را تشخیص می‌دهند، اما چون توانی ارسال نمی‌کنند 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 می‌دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده‌ای می‌شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می‌توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس‌های 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.