امنیت در شبکه‌های محلی بی‌سیم

(Wireless LAN Security)

علیرضا صالحی

اشاره

شبکه‌های محلی بی‌سیم (Wireless Local Area Network: WLAN) را می‌توان در اغلب سازمان‌های بزرگ مشاهده کرد. امروزه ارزش شبکه‌های بی‌سیم بر کسی پوشیده نیست و برپایی این قبیل شبکه‌ها ضمن به همراه آوردن امکانات مطلوب، کاهش هزینه‌ها را نیز در پی دارد. اما هرچه بر عمومیت و محبوبیت این شبکه‌ها افزوده می‌شود دو نکتهٔ مهم یعنی مدیریت و امنیت، بیش از پیش اهمیت خود را نشان می‌دهد. به خصوص در سازمان‌های بزرگ که مساله امنیت بسیار حائز اهمیت است، نوع خطراتی که این شبکه‌ها را تهدید می‌کند و نحوه مقابله با آن‌ها اهمیتی حیاتی دارد.

اقدامات امنیتی اولیه باید به نحوی انجام گیرند که مزایای شبکه‌های بی‌سیم همچنان پابرجا و محفوظ بماند و راهکارهای امنیتی آن‌قدر دشوار نباشند که علت وجودی شبکه بی‌سیم را زیر سوال ببرند. به همین منظور در این نوشتار ابتدا مبانی شبکه‌های محلی بی‌سیم مورد بررسی قرار می‌گیرند و در ادامه نحوه مقابله با انواع خطراتی که چنین شبکه‌هایی را تهدید می‌کنند، مرور خواهد شد. لازم به ذکر است که در این متن هر جا از «شبکه بی‌سیم» نام برده شده است، مقصود «شبکه محلی بی‌سیم» بوده است.

فناوری شبکه‌های بی‌سیم

فناوری بی‌سیم در سال‌های اخیر به نحو شگرفی رشد کرده است تا حدی که امروزه به عنوان یکی از راه‌حل‌های مناسب جهت سازمان‌های بزرگ مطرح می‌باشد. در واقع رشد تعداد کاربران متحرکی (mobile) که بایستی با شبکه‌های محلی در ارتباط باشند، استفاده از شبکه‌های بی‌سیم را اجتناب‌ناپذیر ساخته است. کاربرانی که در عین داشتن آزادی عمل در جابه‌جایی و تحرک، نیاز به ارتباط online با شبکه محل کار خود را دارند. این کاربران عامل پدید آمدن شبکه‌های دسترسی از دور، موبایل و بی‌سیم بودند. بنابر پیش‌بینی‌ها تا سال ۲۰۰۵ دیگر همراه داشتن ادواتی که قدرت پردازشی و ارتباطی آن‌ها بسیار بیشتر از کامپیوترهای رومیزی فعلی است، تعجب‌آور نخواهد بود.

در این میان، شبکه محلی بی‌سیم که به اختصار به آن WLAN (به جای Wireless Local Area Network) گفته می‌شود از طیف گسترده رادیویی جهت برقراری ارتباط بین سازمان و کاربران متحرک استفاده می‌کند. باند فرکانسی مورد استفاده در این رده کاری برابر ۲/۴ گیگاهرتز می‌باشد که بی‌نیاز از مجوز فرکانسی است. این باند فرکانسی برای چنین ارتباطاتی اختصاص یافته و به صورت دوطرفه عمل می‌کند.

البته برخی ادوات بی‌سیم دیگر از باند فرکانسی ۵ Ghz استفاده می‌کنند. از آن‌جایی که این روش ارتباطی، شیوه‌ای بسیار مناسب و کارآمد است، مؤسسه مهندسان برق و الکترونیک آمریکا (IEEE) طی چندین استاندارد، مشخصه‌های چنین شبکه‌هایی را تبیین نمود و تحت عنوان خانواده 802.11 آن‌ها را معرفی کرد. این مجموعه استاندارد دارای زیربخش‌هایی به شرح زیر است:

IEEE 802.11b

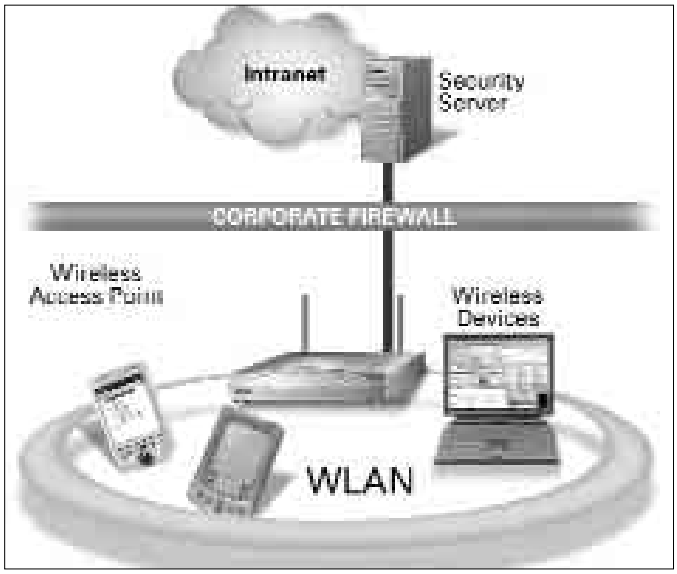
دستگاه‌هایی که این استاندارد را رعایت می‌کنند جهت کار در باند فرکانسی ۲/۴ گیگاهرتز و سرعت انتقال ۱۱ مگابیت در ثانیه در فواصل حدود ۵۰ تا ۱۰۰ متر طراحی شده‌اند. بسیاری از سازندگان معتبر تجهیزات شبکه بی‌سیم از این استاندارد پیروی می‌کنند و در حال حاضر اغلب سازمان‌ها از آن سود می‌برند. از آن‌جایی که مشخصه‌هایی که در این استاندارد تعریف شده‌اند، بسیار کم اشکال و پایدار هستند، توصیه می‌شود که در سازمان‌های بزرگ از آن استفاده شود.

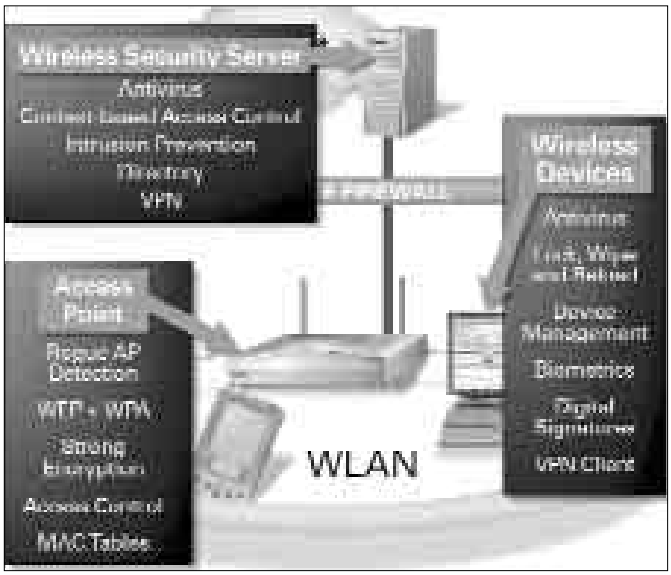
البته به علت تعداد زیاد استفاده‌کنندگانی که در باند ۲/۴ Ghz عمل می‌کنند، امکان تداخل بین دستگاه‌های آن وجود دارد، ضمن آن که 802.11b فقط از ۳ کانال ارتباطی (از مجموع ۱۱ کانال) روی این باند استفاده می‌کند. شیوه ارتباطی نیز DSSS (طیف گسترده رشته‌ای مستقیم) است (جهت آشنایی با این شیوه به شماره ۲۶ ماهنامه شبکه ـ ویژه‌نامه شبکه‌های کامپیوتری مراجعه فرمایید).

IEEE 802.11g

این مشخصه نیز مربوط به باند فرکانسی ۲/۴ Ghz است ولی جهت کار با سرعت ۲۲ مگابیت بر ثانیه در مسافت‌های ۳۰ الی ۷۰ متری. هرچند که سرعت این استاندارد در حد ۲۲ مگابیت تعریف شده است، اما پیاده‌سازی آن بسیار گران‌قیمت بوده و به همین علت در کاربردهای محدودتر نظیر بازار ادوات SOHO (Small Office/Home Office) مورد استفاده قرار می‌گیرد.

شکل ۱ ـ دسترسی به اینترنت را می‌توان برای کاربران شبکه بی‌سیم مهیا نمود، اما بهتر است این کار با استفاده از یک فایروال و سرور امنیتی صورت گیرد.





شکل۲- جهت حفاظت شبکه در تقابل از نفوذی‌های غیرمجاز وحملات ویروسی، لازم است که هر یک از اجزای شبکه تدابیر امنیتی خاصی را اتخاذ کنند.

IEEE 802.11a

این استاندارد جهت دستگاه‌هایی تعریف شده است که در باند فرکانسی ۵ Ghz عمل می‌کنند و میزان گذردهی ۵۴ مگابیت بر ثانیه را در محدوده ۱۰ تا ۳۰ متری پوشش می‌دهند. 802.11a استفاده از ۱۲ کانال را مجاز شمرده است. سرعت بسیار بالاتر دستگاه‌هایی که از این استاندارد پشتیبانی می‌کنند، برای کاربرانی که به چنین سرعتی نیاز دارند، مناسب است اما محدودیت فاصله آن نیز باید در نظر گرفته شود، ضمن آن که همچنان پیاده‌سازی آن گران بوده و استفاده از آن در همه مکان‌ها مقرون به صرفه نیست. البته سازمان‌هایی هستند که تمامی این هزینه‌ها را تقبل می‌کنند تا چنین شبکه‌ای را راه‌اندازی کنند و از مزایای سرعت بالا، امکان فعال‌سازی سرویس‌هایی نظیر QoS (کیفیت سرویس) و امنیت بالا بهره ببرند.

IEEE 802.11h

این مشخصه، نوع اروپایی استاندارد 802.11a است که بعضی ویژگی‌ها به آن اضافه گردیده است از جمله: رعایت TPC یا Transmit Power Control که کارت‌های شبکه بی‌سیم را از انتشار بیش از اندازه سیگنال‌های رادیویی منع می‌کند و همچنین پشتیبانی از DFS (Dynamic Frequency Selection) که به کارت‌های شبکه اجازه می‌دهد قبل از اشغال نمودن یک کانال، به رویدادهای رادیویی اطراف خود توجه کنند.

IEEE 802.11i

این استاندارد هنوز در حال بررسی و اعمال تغییرات است و قرار است در آن ویژگی‌های امنیتی تقویت گردد و شیوه‌های رمزنگاری 802.11 بهبود یابد. در ضمن سازمان IEEE سرگرم کار بر روی استانداردهای دیگری نیز هست که هریک دارای ویژگی و کاربرد خاصی هستند. برخی از این استانداردها عبارتند از:

802.11c: جهت بهبود ارتباط دستگاه‌ها با یکدیگر

802.11d: جهت بهبود عمل گردش درشبکه (roaming)

802.11e: جهت اصلاح و بهبود کیفیت سرویس (Quality of Service)

802.11f: جهت تنظیم بهتر دسترسی Access Point ها

زیرساخت WLAN

به طور کلی، شبکه‌های WLAN به عنوان ضمیمه یا بخشی از یک شبکه بزرگ‌تر LAN برپا می‌شوند و بدین طریق کاربران mobile این امکان را می‌یابند که با شبکه اصلی در تماس باشند. اجزای کلی که در شبکه‌های WLAN به کار می‌روند عبارتند از:

ـ Wireless Access Point که به آن نقطه دسترسی یا AP هم گفته می‌شود. این دستگاه عمل روتر را انجام می‌دهد (درحالت انفرادی عمل Switch یا hub را انجام می‌دهد) و فراهم‌کننده دسترسی‌دستگاه‌های بی‌سیم به شبکه بی‌سیم است. APها عموماً در پشت یک فایروال قرار می‌گیرند تا حفاظت بهتری از شبکه به عمل آید و معمولاً از اغلب استانداردهای 802.11 پشتیبانی می‌کنند. بعضی از آن‌ها در ۲ باند عمل می‌کنند (اصطلاحاً Dual band هستند) به این معنی که یکی از باندها به مثلاً 802.11a و دیگری به 802.11b اختصاص یافته است.

ـ Mobile Device که همان واحد متحرکی است که باید ارتباط آن با شبکه برقرار شود. کامپیوترهای کیفی، دستیارهای دیجیتالی (PDA)، Tablet PCها و دستگاه‌هایی نظیر این‌ها، مثال‌هایی از واحدهای متحرک می‌باشند.

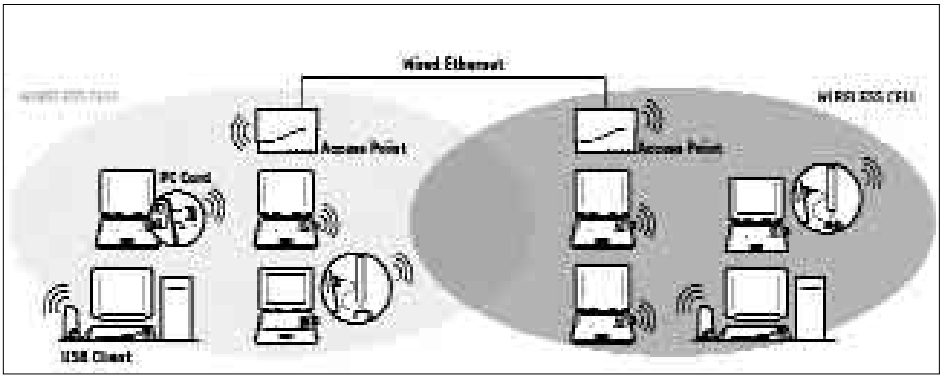
Wireless Network Interface Card یا کارت‌های شبکه بی‌سیم که دستگاه‌های سیار را قادر می‌سازند با AP ارتباط برقرار کنند. هر کارت که همانند کارت شبکه معمولی عمل می‌کند دارای یک آدرس MAC منحصر به فرد است، ضمن آن که لازم است این کارت با AP هماهنگی کامل داشته باشد؛ یعنی به عنوان مثال هر دو در گروه 802.11b باشند. مشابه APها، کارت‌های شبکه بی‌سیم نیز برخی Dual band هستند که مزیت خوبی برای آن‌ها محسوب می‌گردد.

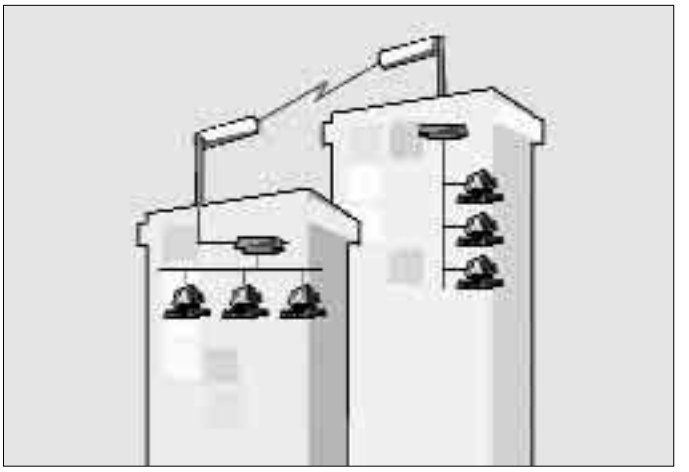
ـ Security Server یا سرور امنیتی. در اغلب شبکه‌های WLAN سروری وجود دارد که مسؤول مدیریت کردن مسایل امنیتی است تا اطلاعات تبادلی روی شبکه آسیب نبینند. این اجزا در شکل‌های یک و دو نمایش داده شده اند.

امنیت در WLAN

مشخصه‌های تعریف شده برای شبکه‌های محلی بی‌سیم به طور ذاتی ناامن هستند زیرا اساساً بنیاد آن‌ها بر این فرض استوار است که همگان باید بتوانند به شبکه دسترسی داشته باشند و از منابع آن استفاده کنند. در نتیجه ویژگی‌های امنیتی باید به مجموعه تعاریف WLAN افزوده شود تا برای سازمان‌های بزرگ قابل استفاده باشد. اما اعمالی که نفوذگران ممکن است طی حمله به شبکه‌های WLAN صورت دهند چگونه است؟ برخی از حملات متداول نفوذگران عبارتند از:

شکل ۳ - هرAP محدوده خاصی را تحت پوشش قرار می دهد. کاربران شبکه باید بتوانند به آسانی بین محدوده‌APهای متفاوت حرکت کنند. به این عمل roaming گفته می‌شود.





شکل ۴ - می توان دو شبکهLAN را به صورت بی سیم به یکدیگر متصل نمود. به این نحوه ارتباط Point to Point: PtP یا نقطه به نقطه گفته می شود.

- Sniffing

این اصطلاح هنگامی به کار می‌رود که شخص مشغول نظارت بر ترافیک شبکه (به طور قانونی یا غیرقانونی) باشد. اغلب اطلاعات ارسالی توسط Access Pointها به راحتی قابل sniff کردن است زیرا فقط شامل متون معمولی و رمز نشده است. پس خیلی آسان است که نفوذگر با جعل هویت دیجیتالی یکی از کاربران شبکه، به داده‌های ارسالی یا دریافتی AP دسترسی پیدا کند.

- Spoofing

این اصطلاح هنگامی استفاده می‌شود که شخصی با جعل هویت یکی از کاربران مجاز، اقدام به سرقت داده‌های شبکه بنماید. به عنوان مثال، فرد نفوذگر ابتدا با sniff کردن شبکه، یکی از آدرس‌های MAC مجاز شبکه را به دست می‌آورد، سپس با استفاده از آن، خود را به عنوان یکی از کاربران معتبر به AP معرفی می‌نماید و اقدام به دریافت اطلاعات می‌کند.

- Jamming

این اصطلاح به معنای ایجاد تداخل رادیویی به جهت جلوگیری از فعالیت سالم و مطمئن AP است. از این طریق فعالیت AP مختل شده و امکان انجام هیچ‌گونه عملی روی شبکه میسر نخواهد شد. به عنوان نمونه، دستگاه‌های منطبق بر 802.11b (به جهت شلوغ بودن باند فرکانسی کاری آن‌ها)به سادگی مختل می‌شوند.

- Session Hijacking

در این جا فرد نفوذگر خود را دستگاهی معرفی می‌کند که ارتبا طش را با AP از دست داده و مجدداً تقاضای ایجاد ارتباط دارد. اما در همین حین، نفوذگر همچنان با شبکه مرتبط بوده و مشغول جمع آوری اطلاعات است.

- Denial of Service

این اصطلاح هنگامی به کار می‌رود که نفوذگر وارد شبکه شده است و ترافیک شبکه را با داده‌های بی‌ارزش بالا می‌برد تا حدی که شبکه به طور کلی از کار بیفتد یا اصطلاحاً Down شود. یکی از راه‌های سادهٔ این کار، ارسال درخواست اتصال به شبکه (Log on) به تعداد بی‌نهایت است.

- Man in the Middle

در این حالت، فرد نفوذگر اقدام به تغییر پیکربندی ادوات متحرک به همراه شبیه‌سازی وضعیت Access Point می‌نماید. در نتیجه ترافیک شبکه به محل دیگری که در آن AP شبیه‌سازی شده، انتقال می‌یابد. در چنین وضعیتی، نفوذگر می‌تواند کلیه اطلاعات را بدون نگرانی و واسطه بخواند و جمع آوری کند، ضمن آن که کاربران همگی فکر می‌کنند که مشغول کار در شبکه خودشان هستند. انجام این کار چندان مشکل نیست زیرا تمامی شبکه‌های WLAN از احراز هویت در سمت سرویس گیرنده (Client-Side authentication) استفاده می‌کنند و احراز هویتی در سمت AP صورت نمی‌گیرد. در نتیجه، کاربران از اتصال به AP مجازی یا غیرمجاز مطلع نمی‌شوند.

با توجه به آنچه توضیح داده شد و ضعف‌های امنیتی فراوانی که مشخصه‌های بنیادین WLANها دارند، سازمان‌ها و نهادهایی همچون IEEE و Wi-Fi ویژگی‌های امنیتی متعددی را برای WLAN پیشنهاد واستاندارد نموده‌اند.

Wired Equivalent Privacy: WEP

مشخصهٔ 802.11b نوعی روش رمزنگاری اولیه به نام WEP دارد که در حالت پیش‌فرض، غیرفعال است. WEP از فرمول RC-4 و۴۰ بیت برای رمز نمودن اطلاعات استفاده می‌کند که با ابزارهای قفل‌شکن امروزی، طی چند ثانیه رمز آن گشوده می‌شود. در نسخه‌های جدیدتر WEP از رمزنگاری ۱۲۸ بیتی استفاده می‌گردد که بسیار بهتر از حالت قبل است اما همچنان کافی نیست.

نقیصهٔ امنیتی که در این‌جا دیده می‌شود فقط در نحوه رمزنگاری نیست، بلکه در مورد کلیدی (Key) است که از آن برای رمزگشایی استفاده می‌گردد ؛زیرا این کلید حالتی ایستا دارد؛ به این معنی که کلید رمزگشا برای همه داده‌های تبادلی در طی زمان ثابت و یکسان باقی می‌ماند و در نتیجه شرایط برای نفوذگر مهیا می‌گردد. اغلب سرپرستان شبکه‌های WLAN هر چند ماه یک بار اقدام به تعویض کلید می‌کنند زیرا ارسال کلید جدید روی شبکه کار آسانی نیست و لازم است که تنظیمات همهٔ APها را به طور دستی تغییر دهند.

اگر در شبکه WLAN حالت رمزگشایی ۴۰ بیتی برقرار باشد، یک نفوذگر به آسانی با گرفتن چندین فریم از داده‌های ارسالی می‌تواند طی چند ثانیه به کلید اصلی دست پیدا کند. حتی اگر از حالت ۲۵۶ بیتی نیز استفاده گردد، باز هم نفوذگر قادر به رمزگشایی پیام‌ها می‌باشد ولیکن به مدت زمان بیشتری برای جمع آوری تعداد زیادتری از فریم‌ها نیاز خواهد داشت.

WEP همچنین دارای ویژگی‌های احراز هویت (از نوع ساده) نیز هست و کاربران جهت دسترسی به شبکه به یک Service Set Identifier: SSID نیاز دارند که عبارت است از یک رشته ۳۲ کاراکتری منحصر به فرد که به ابتدای بسته‌های داده‌ای WLAN الصاق می‌گردد. این کار بدین منظور صورت گرفته که شبکه مطمئن شود فقط بسته‌هایی که دارای این مشخصه هستند مجاز به دسترسی می‌باشند. البته به دست آوردن SSID نیز برای نفوذگران کار آسانی نیست.

Access Pointهای شبکه در ضمن، دارای جدولی از آدرس‌های MAC مجاز شبکه می‌باشند که به احراز هویت کارهای شبکه کمک می‌کند.

همان‌گونه که گفته شد، در حالت پیش‌فرض، ویژگی‌های WEP غیرفعال است. نخستین کاری که سرپرست شبکه WLAN باید انجام دهد فعال کردن آن است تا حداقل راه ورود نفوذگرانی که فقط به دنبال شبکه‌های فاقد ویژگی‌های امنیتی می‌گردند را سد کند. نکته دیگری که باید در این مورد گفته شود نیزاین است که اغلب APها برای اختصاص آدرس IP از پروتکل DHCP (Dynamic Host Configuration Protocol) استفاده می‌کنند و به طور پویا به دستگاه‌های بی‌سیم که قصد اتصال به شبکه را دارند، آدرس‌های IP اختصاص می‌دهند. این مورد نیز از جمله راه‌های ورود غیرمجاز نفوذگران به داخل شبکه است.

سازمان IEEE در کنار ویژگی‌های WEP، تعاریف و مشخصه‌های امنیتی دیگری را نیز برای شبکه‌های WLAN در نظر گرفته است که در کنار رمزنگاری‌های ۱۵۴ بیتی و ۲۵۶ بیتی، کار احراز هویت کاربران را کارآمدتر می‌نماید.

IEEE 802.1x

برای بهینه کردن سیستم احراز هویت در شبکه‌های WLAN سازمان IEEE در حال تدوین استانداردهای 802.1x است. حرف x نشان‌دهنده آن است که هر کدام از سازندگان تجهیزات می‌توانند روش خاص خود را جهت کنترل در این استاندارد اعمال کنند. 802.1x از پروتکل EAP به این منظور استفاده می‌کند.

Extensible Authentication Protocol یکی از پروتکل‌های عمومی برای احراز هویت است که از شیوه‌هایی نظیر: کارت‌های token، روش Kerberos، روش کلید عمومی، روش گواهینامه (Certificate) و روش One-time Password پشتیبانی می‌کند. 802.1x IEEE مشخص می‌کند که EAP چگونه باید در فریم‌های شبکه LAN قرار گیرد.

۳ عضو اصلی شبکه که در 802.1x ملزم به انجام امور امنیتی هستند، عبارتند از: دستگاه‌های بی‌سیم، Access Point و Authentication Server .

سرورِ احراز هویت شامل یک کامپیوتر سرور است که مدیریت امور امنیتی را برعهده دارد. شیوه کار آن نیز به این شرح است:

۱ـ یک کاربر تقاضای اتصال به شبکه WLAN را از طریق Access Point اعلام می‌نماید.

۲ـ Access Point درخواست کاربر را اعتبارسنجی نموده و آن را جهت تایید به سرور احراز هویت که از پروتکلی نظیر RADIUS استفاده می‌نماید، ارسال می‌کند.

۳ـ سرور از AP دلایلی را جهت مجاز بودن کاربر درخواست می‌کند. AP این درخواست را باز کرده و آن را با فرمت EAPOL (EAP encanpsulation over LAN) به کاربر می فرستد.

۴ـ کاربر به محض دریافت چنین بسته‌ای، دلایل معتبر بودن خود را از طریق AP به سرور باز می‌فرستد.

۵ـ سرورِ احراز هویت در صورت صحت داده‌ها، اجازه ورود کاربر را صادر می‌کند. هرچند که این استاندارد، انجام امور اضافه‌ای را بر کاربر و AP تحمیل می‌کند ولیکن به جهت استفاده از شیوه‌های گوناگون رمزنگاری و استفاده از کلید پویا که مرتبا در حال تغییر است، امنیت خوبی را در شبکه برقرار می‌نماید.

IEEE 802.11i و دسترسی محافظت شده

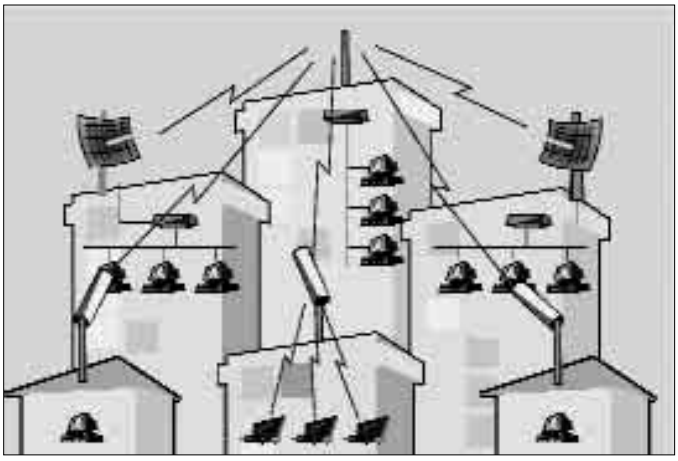
یکی دیگر از استانداردهایی که IEEE در حال حاضر مشغول تکمیل آن است نسخه 802.11i می‌باشد. در این نسخه از پروتکل TKIP (Temporal key Integrity Protocol) استفاده می‌شود که می‌تواند به طور پویا کلیدهای WEP را پس از ارسال ۱۰ هزار Packet تغییر دهد. نسخه فعلی از کد ۴ رقمی استفاده می‌کند که قرار است در نسخه‌های بعدی از AES استفاده شود.

دسترسی محافظت شده به شبکه بی سیم که با عنوان WPA (Wireless Protected Access) شناخته می‌شود یکی از شیوه‌های مطلوب محافظت از شبکه است که در این استاندارد گنجانده شده و اغلب دستگاه‌هایی که از استاندارد Wi-Fi پشتیبانی می‌کنند آن را در خود جای داده‌اند.

WPA از تعدادی الگوریتم ریاضی برای احراز هویت کاربران استفاده می‌کند. اگر کاربری ۲ Packet غیرمجاز را طی یک دوره زمانی (مثلاً یک ثانیه) ارسال کند، سیستم فرض می‌کند که شبکه مورد حمله قرار گرفته است در نتیجه، به طور خودکار کلیه راه‌های دسترسی را مسدود می‌کند. فعال‌سازی این ویژگی فقط برای سازمان‌هایی که از درجه امنیت بسیار بالایی برخوردار ند، توصیه می‌شود.

Access Pointهای تقلبی

یکی دیگر از شیوه‌های نفوذ به درون شبکه‌های WLAN استفاده از APهای



شکل ۵ـ شبکه‌های WLAN را می توان به صورت Point-to-multipoint هم راه اندازی نمود. به این صورت می توان چندین شبکه LAN فرعی که ممکن است خودشان بی سیم باشند را به یک نقطه مرکزی متصل نموده وشبکه محلی بی سیم بزرگتری تشکیل داد.

غیرمجاز یا تقلبی است. نفوذگران می‌توانند با اتصال یک AP که مشخصاتی مشابه مشخصات APهای درون شبکه دارد، خود را وارد ترافیک شبکه نمود و همانند اعضای معمولی به دریافت اطلاعات بپردازند. یکی از راه‌های مقابله با این شیوه، استفاده از آشکارسازهای امواج رادیویی است. به این منظور باید اشخاصی به طور فیزیکی در اطراف ساختمان محل استقرار شبکه بی‌سیم حرکت کرده و با استفاده از این آشکارسازها، APهای احتمالی را کشف کنند. حتی ممکن است چنین AP هایی توسط کارمندان ناراضی در داخل همان ساختمان نصب شده باشند، لذا یافتن آن‌ها کاری حساس و دشوار است.

مبحث شیوه‌های نفوذ به شبکه‌های Wireless و نحوه مقابله با آن‌ها بسیار گسترده است و هر روز نیز بر اهمیت و پیچیدگی آن افزوده می‌گردد. توضیحات بیشتر درباره مطالب مطرح شده در این مقاله را می‌توانید در کتاب‌های مربوط به این رشته و سایت‌هایی که در کادر «سایت‌های مفید» آورده شده‌اند، مطالعه نمایید. همچنین درباره استاندارد 802.11g در مقاله دیگری به تفصیل سخن خواهیم گفت. اما سازمان‌ها برای حفظ امنیت شبکه‌های خود چه می‌توانند بکنند؟

همان‌گونه که قبلاً گفته شد، سازمان‌های بزرگ بهتر است از IEEE 802.11b و محصولاتی که آن را پشتیبانی می‌کنند، استفاده نمایند. توصیه‌های ذیل شامل رعایت مبانی مسایل امنیتی است و حداقل‌های لازم برای این کار را بیان می‌دارد:

۱ـ دیدگاه خود را متناسب با اندازهٔ سازمان تغییر دهید؛ یعنی هنگام توسعه و مدیریت امنیت شبکه، نیاز سازمان را مدنظر قرار دهید.

۲ـ هدف از ایجاد شبکه WLAN را به روشنی مشخص کنید. ضعف امنیتی ذاتی شبکه‌های WLAN نباید شما را از استفاده از آن‌ها منصرف کند ولی به یاد داشته باشید که هرگز برای کارهای بسیار حساس و حیاتی از آن استفاده نکنید. این شبکه‌ها برای ساده کردن امور جاری سازمان مناسب هستند و بهتر است در همان حوزه‌ها مورد استفاده قرار گیرند.

۳ـ کاربران شبکه را به دقت مشخص کنید. واضح است که اگر در تعیین هویت کاربران و مشخص نمودن آن‌ها کوتاهی کنید، هیچ کدام از شیوه‌های امنیتی نمی‌توانند به سادگی جلوی خرابکاری کاربران غیرمجاز را بگیرند.

۴ـ سرمایه‌گذاری مناسبی انجام دهید.

در انتخاب سخت‌افزار و نرم‌افزارهای مناسب شبکه با توجه به کاربردهای مورد نیاز سرمایه‌گذاری کنید و از هزینه کردن نهرا سید.

۵ـ از همه ویژگی‌های امنیتی WLAN استفاده کنید. برای این منظور این ویژگی‌ها را در نظر داشته باشید:

الف ـ مطمئن شوید که WEP روی APها فعال شده است به خصوص هنگامی که APها را reset می‌کنید.

ب ـ همواره فهرست روزآمدی از آدرس‌های MAC در اختیار داشته باشید.

ج ـ از انتشار SSID جلوگیری کنید و آن را فقط برای کاربران احراز هویت شده ارسال نمایید. در ضمن تعداد SSID را از تعداد پیش‌فرض آن که برای کلیه محصولات یک کارخانه یکسان است، تغییر دهید.

د ـ حتی‌الامکان از DHCP روی APها استفاده نکنید.

ه ـ از ویژگی‌های WPA روی کلیدهای WEP استفاده کنید.

و ـ اگر می‌توانید برای ایجاد یک ارتباط امن از VPN استفاده کنید. البته پیاده‌سازی Virtual Private Networks یا VPN در حال حاضر گران‌قیمت است ولی تا امروز امن‌ترین حالت ارتباطی در شبکه‌های بی‌سیم محسوب می‌شود. استفاده از فایروال نیز توصیه می‌شود.

ز ـ تازه‌های فناوری WLAN را زیر نظر داشته باشید. تا ازمحصولات جدیدی که می‌توانند در بهبود شبکه شما مؤثر باشند، غافل نشوید.

ح ـ به جای هر فصل یک بار، هر ماه یک بار در حوزه فیزیکی شبکه قدم بزنید و نسبت به کشف APها یا سایر ادوات غیرمجاز اقدام کنید. این کار را به آسانی می‌توانید با استفاده از یک کامپیوتر همراه و ویندوز XP انجام دهید.

ط ـ مشاوران خوبی انتخاب کنید. بدون شک دارا بودن شبکه بی‌سیم و استفاده بهینه از آن نیازمند مشاوره با متخصصان این فن است. آموزش مناسب کاربران را نیز از یاد نبرید.

سایت‌های مفید

سازمان مهندسان برق و الکترونیک آمریکا	www.ieee.org
بخش مربوط به WLAN در سازمان IEEE	grouper.ieee.org/groups/802/
سایت Wi-Fi شرکت مایکروسافت	www.microsoft.com/wifi
درباره طیف رادیویی گسترده	www.sss-mag.com
خودآموز 802.11	www.80211-planet.com/tutorials
فرهنگ لغات مرتبط با شبکه و فناوری	www.webopedia. com