بسمه تعالی



**وزارت علوم ، تحقیقات و فن آوری**

**دانشکده فنی پسران تبریز**

**پروژه دوره کاردانی**

**ارائه کننده:**

**استاد راهنما:**

**رشته تحصیلی:**

**کامپیوتر گرایش نرم افزار**

**نیمسال 96-95**

**عنوان پروژه:**

**امنیت در شبکه** ‌**های بی**‌**سیم**

**فهرست مطالب:**

**مقدمه**

**1. شبکه‌ های محلی بیسیم**

**2. سطح پوشش WLAN**

**3. سرویس‌های امنیتی 802.11b و Integrity**

**4. خطرها و حملات امنیتی**

**5. ده نکته اساسی در امنیت شبکه های WI-FI**

## 6. دو تفکر اشتباه در مورد امنیت شبکه‌های بی‌سیم

## نتیجه گیری

## منابع

**مقدمه:**

از آن‌جا که شبکه‌ های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ‌ها، که بر اساس سیگنال ‌های رادیویی‌ اند، 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 آن‌ ها که به ‌مدد پیکربندی صحیح می‌توان به‌ سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه ‌ها با تأکید بر ابعاد امنیتی آن ‌ها، به روش ‌های پیکربندی صحیح که احتمال رخ داد حملات را کاهش می‌دهند بپردازیم.

**1) شبکه‌ های محلی بی‌سیم**

تکنولوژی و صنعت WLAN به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌ های محلی‌ بی‌سیم به کندی صورت می ‌پذیرفت. با ارایه‌ ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه‌ های محلی امکان‌پذیر می‌ ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل‌ها و استانداردهای خانواده‌ی IEEE 802.11 است.

اولین شبکه‌ی محلی بی ‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه ‌ها، هزینه‌ای بالا و پهنای باندی پایین را تحمیل می ‌کرد که ابداً مقرون به ‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی 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 پایه‌ی این استاندارد ها 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 به ‌تاز‌ه‌گی 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 شبکه‌ های بی ‌سیم آرام آرام در حال گسترش است.

**معماری‌ شبکه‌ های محلی‌ بی‌سیم**

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

    معماری‌ معمول در شبکه‌ های محلی‌ بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان 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 می‌دهد را BSS(Basic Service Set) می‌نامند. مجموعه‌ی تمامی سلول ‌های یک ساختار کلی‌ شبکه، که ترکیبی از BSS های شبکه است، را ESS(Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ ی وسیع ‌تری را تحت پوشش شبکه‌ی محلی‌ بی‌سیم درآورد.

    در سمت هر یک از سخت ‌افزارها که معمولاً مخدوم هستند، کارت شبکه ای مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه ‌ی بی‌سیم، به بستر پرسرعت ‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌ های مجهز به کارت شبکه‌ ی بی ‌سیم و شبکه ‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :

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



 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 ای به عنوان خادم 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.

**مزایا شبکه های محلی**

**مزایا:**

**جابجايي كاربر-** کاربران مي توانند به فايلها، منابع شبكه و اينترنت دسترسي پيدا كنند، بدون اين كه نياز به اتصال شبكه با استفاده از سيم داشته باشند. كاربران در حال حركت نيز مي توانند همان سرعت بالا و دسترسي بلادرنگ خود به تجهيزات شبكه ي محلي را حفظ كنند.

**نصب سريع-**  زمان مورد نياز براي نصب كاهش م ييابد، زيرا اتصالات شبكه نياز به اضافه كردن يا جابجايي سيم يا تغيير در زيرساخت را ندارد.

**انعطاف پذيري-** سازما نها مي توانند به راحتي شبكه هاي محلي بي سيم را نصب يا قطع كنند. در مواقع لازم مانند كنفرانس ها يا نشست ها، امكان نصب سريع و موقتي يك شبكه ي محلي كوچك وجود دارد.

**مقياس پذيري-** توپولوژي هاي شبكه هاي محلي بي سيم به آساني و براي هر كاربرد خاص قابل تنظيم است. همچنين، اين شبكه ها از يك شبكه ي نظير به نظير كوچك تا شبكه هاي سازماني خيلي بزرگ قابل توسعه است.

معایب:

یکی از مهمترین این مشکلات سرعت انتقال داده در این شبکه‌هاست.

مساله دیگر امنیت در شبکه‌های وایرلس است. این شبکه‌ ها خیلی آسان‌ تر از شبکه‌های کابلی می توانند مورد دستبرد قرار بگیرند. استاندارد های جدید روشهای کدگذاری جدیدی معرفی می کنند تا امنیت این شبکه‌ها را بالا ببرند. اما روشهای کدگذاری سرعت انتقال را کاهش می‌دهد.

2) **سطح پوشش WLAN**

    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 قدرت‌ مندی 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 کلی ای که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عملکرد مقداری‌ است که برای محل‌های بسته و ساختمان ‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

    شکل زیر مقایسه‌ای میان بردهای نمونه در کاربردهای مختلف شبکه‌ های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :



    یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ ‌های بی‌سیم، عمل اتصال میان حوزه ‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌ های بی‌سیم را به‌دست‌ آورد.

    اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه ‌به ‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌ های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

    نقاط دسترسی ای که به عنوان پل ارتباطی میان شبکه‌ های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌ معنای شعاع پوشش بالاتر است. این سخت ‌افزارها 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، فاصله‌ای متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌ های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد.

     شکل زیر نمونه ای از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می‌دهد :



**3)سرویس‌ امنیتی 802.11b و Integrity**

   در استاندارد 802.11b، از تکنیک ‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. 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 سیاست ‌های امنیتی در شبکه‌ های محلی  بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن ‌سازی 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 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 شبکه‌ های محلی بی ‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌ های 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 آسیب ‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

 **Integrity**

    مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی ای 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 مخدوم‌ های بی ‌سیم و نقاط دست‌رسی کم می‌ شود. روش مورد نظر استفاده از یک کد CRC است. همان ‌طور 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 داده های 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 اندازه‌ ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

     متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلید های امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی ‌سیم را نصب می‌کنند به ‌صورت دستی پیاده‌ سازی 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 شبکه‌ های بی ‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری ‌های انجام ‌شده از سوی کاربران و مدیران شبکه مانند تغییر ندادن کلید به‌صورت مداوم، لو دادن کلید، استفاده از کلیدهای تکراری یا کلید های پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌ های بی‌ سیم ندارد. این مشکل از شبکه‌ های بزرگتر بیشتر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخ‌داد چنین سهل ‌انگاری ‌هایی، زمانی که تعداد مخدوم‌ های شبکه از حدی می‌گذرد عملاً کنترل‌ کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

**4)خطرها و حملات امنیتی**

  با توجه به پیشرفت های اخیر، در آینده ای نه چندان دور باید منتظر گسترده گی هرچه بیشتر 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 802.11bمی 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 محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

**1- 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.

**2- 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 معنا داری 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 :

**3-  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.

**4- 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.

**5- تغییر پیام**

    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.

**6- 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 سوء استفاده از اختلال ایجاد شده به نفوذ از طریق همان سرویس نیز اقدام کند.

**5) ده نکته اساسی در امنیت شبکه های WI-FI**

**۱ – کلمه عبور پیش‌فرض سرپرست را تغییر دهید**

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

**۲ – رمزگذاری WPA/WPA2 را فعال کنید**

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

**۳ – SSID پیش‌فرض را تغییر دهید**

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

**۴ – فیلترگذاری آدرس MAC را فعال کنید**

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

**۵ – SSID Broadcast را غیرفعال کنید**

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

**۶ – به‌طور خودکار به شبکه‌های وای‌فای باز متصل نشوید**

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

**۷ – به ابزارهای خود آدرس‌های IP ثابت اختصاص دهید**

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

**۸ – فایروال‌ها را روی هر کامپیوتر و روتر فعال کنید**

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

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

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

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

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

## (6دو تفکر اشتباه در مورد امنیت شبکه‌های بی‌سیم

**۱- استفاده از رمزنگاری نوع WEP**

شاید در مورد رمزنگاری شبکه های بی سیم اطلاعات زیادی نداشته باشید . اما به صورت کلی باید گفت که هرچه رمزنگاری یک شبکه قوی تر باشد ، عبور کردن از سدهای امنیتی آن مشکل تر می شود . اما همه انواع رمزنگاری نیز باعث امنیت بیشتر شبکه های بی سیم نمی شوند . رمزنگاری نوع WEP یکی از همین نوع رمزنگاری هاست که به راحتی دور زده می شود .

در روترهایی که امروزه فروخته می شوند ، امکان استفاده از رمزنگاری WEP نیز وجود دارد . اما این قابلیت بیشتر برای دستگاه هایی قرار داده شده است که قدیمی هستند و امکان استفاده از روش های رمزنگاری جدید مثل WPA و WAP2 را ندارند . پس اگر دستگاه شما مشکلی در پشتیبانی از روش های رمزنگاری های جدید ندارد ، حتما به جای استفاده از WEP از WPA یا WPA2 استفاده کنید ( ترجیحا از WPA2 استفاده شود .



**-2  استفاده از کلمات عبور ضعیف**

همه می دانند که استفاده از کلمات عبور ساده و قابل حدس بسیار خطرناک است . شاید فکر کنید که استفاده از روش رمزنگاری WPA2 باعث امنیت کامل شما خواهد شد . اما حتی اگر از WPA2 نیز به منظور رمزنگاری استفاده کنید ولی کلمه عبورتان ضعیف باشد ، هیچ تاثیری در افزایش امنیت شما نخواهد داشت .

سعی کنید که کلمه عبور شبکه بی سیم تان کمتر از ۸ کراکتر نباشد . چون با استفاده از حملات ” دیکشنری ” که بر پایه حدس زدن ترکیب کلمات ، اعداد و نشانه ها کار می کنند ، به راحتی در هم می شکنند . بهتر است که کلمه عبورتان بین ۱۵ تا ۲۰ کراکتر باشد . همچنین این کلمه عبور باید ترکیبی از حروف بزرگ و کوچک ، اعداد و نشانه ها باشد تا حدس زدن آن تقریبا غیر ممکن شود .

**نتی****جه گیری**

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

**منابع** **:**

* سایت آشیانه ( گروه امنیتی )( www.ashiyane.org)
* سایت مجله شبکه های کامپیوتری (www.shabakeh-mag.com)
* سایت خبری (www.isna.ir)