معرفی مفاهیم شبکه های وایرلس قسمت ۲ : SSID ، احراز هویت و آنتن ها (نسخه PDF)

شبکه هایی که به عنوان مکملی در کنار شبکه های کابلی، نقش مهمی در شبکه های بروز و سناریوهای پیچیده امروزی دارند و هک کردن چنین شبکه هایی نیازمند راه کارها و روش های مخصوص بخود است. همانطور که در مباحث قبلی هم ذکر شد، در یادگیری هک، همیشه حرف اول را یادگیری و درک مفاهیم پایه میزند و پس از شناخت صد در صدی محیط مورد نظر، روش های هک کردن و تست نفوذ گرفتن از آن مطرح خواهد شد.بنابراین در ادامه صحبت های گفته شده، سعی خواهم کرد مبحث مفاهیم شبکه های وایرلس را در دو بخش خدمت شما ارائه کنم که بخش اول آن را در همین مقاله مطالعه خواهید نمود.

یک شبکه وایرلس، سیستمی راحت و منعطف از تبادل دیتاست که از تکنولوژی فرکانس رادیو بهمراه رسانه وایرلس برای ارتباط استفاده میکند و دیتا را از طریق هوا بدست میآورد. این شیوه کاربر را از ارتباطات کابلی مختلف و پیچیده میرهاند. این تکنولوژی با استفاده از امواج الکترومغناطیس، اطلاعات را از یک نقطه به نقطه دیگر بدون دخالت عوامل انسانی ربط میدهد. برای درک بهتر مفهوم نفوذ به شبکه های وایرلس، ابتدا باید بخوبی مفاهیم وایرلس را یاد گرفت. در این بخش و بخش اول، دیدی بر شبکه های وایرلس، انواع شبکه های وایرلس، استانداردهای وایرلس، حالات احراز هویت و پردازش، اصطلاح شناسی وایرلس و انواع مختلف آنتن وایرلس خواهیم داشت.

Service Set Identifier (SSID) چیست ؟

SSID یک شناسه منحصربفرد است که برای برقراری و ثبات ارتباط وایرلس استفاده میشود. SSID یک توکن برای شناسایی شبکه ۸۰۲.۱۱ (Wi-Fi) است که بصورت پیش فرض بخشی از هدر بسته ای است که تحت WLAN ارسال میشود. این توکن به عنوان یک پسورد مشترک بین اکسس پوینت ها و کلاینت ها عمل میکند. نگرانی امنیتی زمانی بالا میرود که مقدار پیش فرضSSID تغیر نکرده باشد؛ در این صورت شبکه حاصله بشدت مورد تهدید قرار میگیرد.اکسس پوینت های SSID، بصورت پیوسته سیگنالهای رادیویی را از خود منتشر میکنند که اگر قابلیت مربوطه بر روی ماشین های کلاینت فعال باشد، آن را دریافت خواهند کرد. روش های غیر امن در Station به این صورت خواهد بود که با اکسس پوینت ها از طریق انتشار SSID ساختاربندی شده، SSID خالی و یا SSID ای که با حالت"Any" ساختاربندی شده باشد، مراوده نماید.

- **نکته:** در بحث شبکه های وایرلس، Station به هر دیوایسی گفته میشود که بتواند رفتاری شبیه وایرلس کلاینت از خود نشان دهد. بطور مثال ارتباط با اکسس پوینت های دیگر و یا روترها و .... در اینجا منظور از Station هرگونه دیوایسی است که قابلیت Bridge کردن شبکه وایرلس با رفتاری شبیه یک کلاینت استاندارد را دارد.

به ادامه بحث بر میگردیم. از آنجایی که SSID یک نام خاص است که به هر شبکه وایرلس داده میشود، تمام دیوایس ها و اکسس پوینت های حاضر در آن شبکه بایستی از SSID یکسان استفاده نمایند. ارائه SSID معتبر برای هر دیوایسی که میخواهد به شبکه وایرلس وارد شود، الزامی است. اگر به هر علتی SSID شبکه تغیر یافت، هر کابری برای ادامه ارتباط خود با شبکه باید تغیرات ایجاد شده را در دیوایس مورد نظر اعمال نماید.متاسفانه SSID اگر در قالب بسته های ارتباطی شنود شود، تمام امنیت خود را از دست داده است. بعبارت دیگراز آنجایی که SSID بصورت رمز نشده منتقل میشود، پس تا زمانی امن است که شنود نشود. یک عبارت SSID میتواند حداکثر تا ۳۲ کارکتر طول داشته باشد. برخی از SSID های معمول را در زیر مشاهده خواهید کرد:

```
comcomcom
Default SSID
Intel
linksys
Wireless
WLAN
```

حالات احراز هویت وای-فای

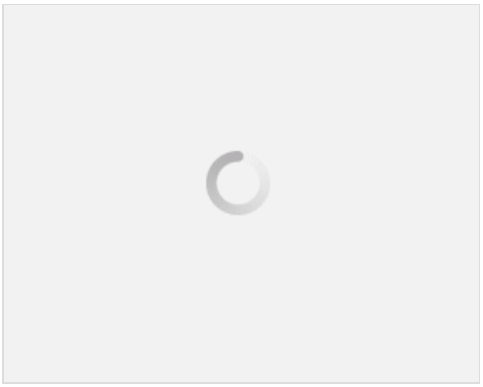
احراز هویت وای-فای میتواند به دو روش انجام شود:

۱. سیستم باز

۲. کلید مشترک

فرآیند احراز هویت در سیستم باز

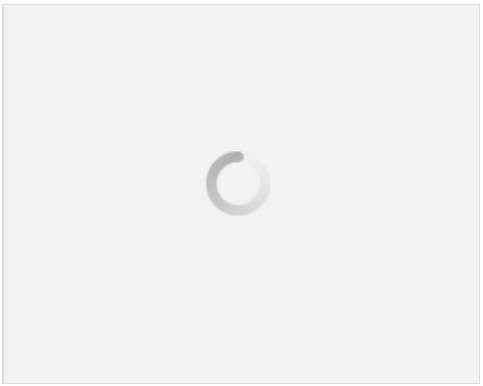
در این حالت، هر کلاینتی میتوانـد جهت احراز هویت، درخواست بفرسـتد. در این فراینـد یک کلاینت میتوانـد یک فریم مـدیریتی احراز هویت که شامل هویت خودش است را برای تائید اعتبار و اتصال به اکسس پوینت بفرستند. اکسس پوینت، SSID کلاینت را چک کرده و در صورت تطـابق آن، در پاسـخ یـک فریم تائیـد اعتبار را به کلاینت (wireless station) بر میگردانـد. کلاـینت به هنگام دریافت این فریم تائیدیه، به شبکه و یا station واسط وصل میشود.



فرآیند احراز هویت در حالت کلید مشترک

در این حالت، به نظر میاید هر Station وایرلسـی بایستی یک کلید مخفی به اشتراک گذاشته شده را از طریق یک کانال امن دریافت کند. این کانال امن از کانال های ارتباطی شـبکه وایرلس تحت استاندارد ۸۰۲.۱۱، متمایز است. مراحل زیر نحوه ایجاد کانکشن را در فرایند کلید مشترک بیان میکند:

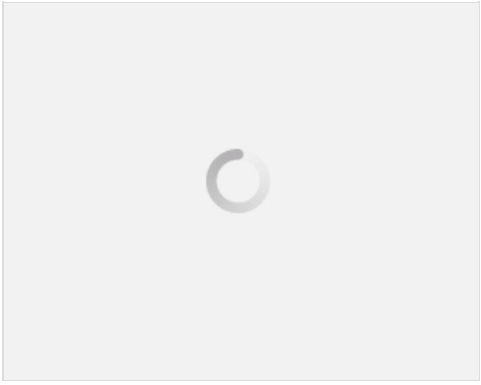
۱. استیشن (کلاینت) درخواست احراز هویت را به اکسس پوینت ارسال میکند.
۲. اکسس پوینت Challenge text را به استیشن (کلاینت) ارسال میکند.
۳. استیشن (کلاینت)، Challenge text را با اسـتفاده از کلیـد پیش فرض ۶۴ یا ۱۲۸ بیـتی خودش رمز میکنـد و متن رمز شـده را به اکسس پوینت بر میگرداند.
۴. اکسـس پوینت از کلید WEP خودش (که منتـاظر بـا کلیـد پیش فرض استیشن (کلاـینت) است) برای رمزگشایی متن رمز شـده اسـتفاده میکند. اکسـس پوینت متن رمزگشایی شده را با متن اصـلی (Challenge text) مقـایسه کرده و در صورت یکسـان بودن، استیشن (کلاینت) را تائید هویت می کند.
۵. استیشن (کلاینت)، به شبکه وصل میشود.



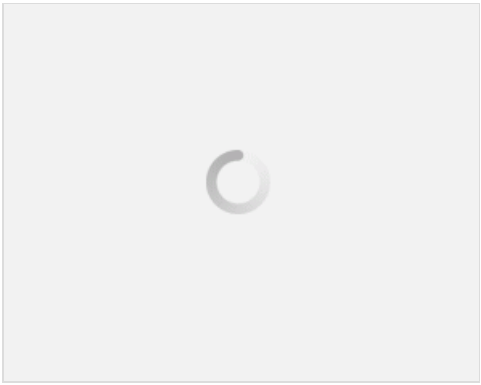
فرایند احراز هویت وای-فای با استفاده از یک سرور مرکزی

استاندارد ۸۰۲.۱x احراز هـویت مرکزی را ایجـاد کرده است. برای اجرایی شـدن این احراز هـویت مرکزی بر روی شـبکه وایرلس، اکسـس پوینت بایستی بتواند بصورت امن ترافیک را از سوی کلاینت های خاص شـناسایی کند. این شـناسایی با استفاده از کلیدهای احراز هویت که به اکسـس پوینت و کلاـینت از طرف RADIUS سـرور ارسال شـده است انجام میشود. اگر کلاینت از رنـج مجاز اکسـس پوینت باشد، مراحل زیر رخ خواهد داد:

۱. کلاینت درخواست احراز هویت را به اکسس پوینت جهت ایجاد ارتباط ارسال میکند.
۲. اکسس پوینت EAP-Request را برای شناسایی کلاینت بر میگرداند.
۳. کلاینت با استفاده از EAP-Response هویت خود را به اکسیس پوینت ارسال میکند.
۴. اکسس پوینت هویت دریافت کرده را از طریق پورت کنترل نشده به RADIUS سرور ارسال میکند.
۵. RADIUS سرور از طریق اکسس پوینت درخواستی مبتی بر نوع مکانیزم استفاده شده را به کلاینت ارسال میکند.
۶. کلاینت با اعتبار خودش از طریق اکسس پوینت جواب را به RADIUS سرور میفرستند.
۷. اگر اعتبار کلاینت مورد قبول واقع شد، RADIUS سرور یک کلید احراز هویت رمز شده را به اکسس پوینت ارسال میکند.
۸. اکسس پوینت یک کلید احراز هویت Multicast/global رمز شده را به کلاینت ارسال میکند.



اصطلاحات و واژه های وایرلس



انواع آنتن های وایرلس

آنتن هـا در ارسـال و دریـافت سـیگنال های رادیو بسـیار مهم و حیاتی هسـتند. آن ها پالس های الکتریکی را به سـیگنال های رادیویی و بلعکس تدیل میکنند. بطور اساسی پنج نوع آنتن وایرلس وجود دارد:

آنتن جهت دار

آنتن جهت دار برای انتشار (Broadcast) و گرفتن امواج رادیویی از یـک جهت بکار میرود. به منظور افزایش کارایی انتقال و دریافت، آنتی های جهت دار طوری طراحی شـده انـد که در جهت های نزدیک بهم در مقایسه با سایر جهات بصورا موثر و کارا فعالیت کنند. این قابلیت باعث کاهش تداخلات نیز میشود.

آنتن چند جهته

آنتن هـای چنـد جهته انرژی الکترو مغنـاطیس را در تمـام جهات و بصورت منظم از خود متساطع میکننـد. آن ها معمولا امواج قـدرتمند

یکسانی را در دو بعد از خود انتشار میدهند، اما این قدرت به اندازه حالت سه بعدی نیست. بهترین مثال برای آنتن های چند جهته، آنتن های مورد استفاده در ایستگاه های رادیویی هستند. این آنتن ها برای انتقال سیگنال های رادیو موثر هستند چرا که گیرنده امواج ممکن است متحرک باشد. در نتیجه رادیو میتواند سیگنال هایش را در جهتی بر خلاف جهت انتن دریافت کند.

آنتن شبکه سهمی‌وار

این آنتن ها بر اساس قاعده دیش های ماهواره ای کار میکنند. این نوع از آنتن ها یک دیش نصفه دارند و دارای یک شبکه که با استفاده از کابل آلومینیومی ایجاد شـده است هسـتند. این آنتن های شـبکه ای سـهمی وار با اسـتفاده از اصل پرتو رادیویی متمرکزشـده میتوانند انتقـال وای-فـای را به فواصل بسـیار دور انجام دهنـد. اساسا این نوع از آنتن ها برای انتقال سـیگنال های ضـعیف رادیویی از میلیون ها کیلومتر دور تر از زمین بکار میروند.

آنتن Yagi

یاگی یک آنتن غیر جهت دار است که در ارتباطات یک باند فرکانسی ۱۰ مگاهرتز به VHF و UHF مورد استفاده قرار میگیرد. این آنتن ها به آنتن های Yagi Uda نیز مشهور هستند.

آنتن دو قطبی

یک دو قطبی، یک هادی الکتریکی مستقیم است که نصف طول موج را اندازه گیری میکند.

سربلند و مانا باشید

پایان بخش دوم

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

حامد خورشید

با تشکر از مقاله.

خوب بود ولی غلط املایی داشت.

احسان امجدی

ممنون دوست عزیز. معمولا در نوشتن مطالب این چنینی و بقول معروف تایپی، وجود چند غلط املایی چیز عجیبی نیست ولی با این حال من همیشه یکبار متن رو بعدش میخونم تا مشـکلی نباشه... حرف شـما صحیحه ولی ایکاش دقیقا میگفتید که مشکل کجاست تا اصلاح کنم. یکبار دیگه متن رو خوندم ولی چیزی ندیدم.

حامد خورشید

با سلام

دوست عزیزم

مفاهمی - در مقاله اول پاراگراف دوم کلمه بیستم

احسان امجدی

حامد جان با اینکه آدرس اشتباه دادی (توی مقاله دوم بود)، ولی اصلاح شد. ممنون از دقت نظرت

حاشا جان ! اینکه آدرس اشتباه داشتی (روی شناسه دوم بود)، ولی اصلاح شد. ممنون از دقت نظرت

+۲۲+****۹

سلام . ممنون از مطالب خوبتون .

مطلب اصلی