امنیت شبکه

جلسه هفتم: امنیت شبکه‌های بی‌سیم

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

- امنیت بی‌سیم
- تهدیدهای شبکه بی سیم
- ایجاد امنیت در انتقالهای بی‌سیم
- نگرانی‌های عمده در مورد تجهیزات بی سیم
- استراتژی امنیت
- مدل معماری و اجزای شبکه IEEE 802.11
- خدمات امنیتی

امنیت بی‌سیم

فاکتورهای کلیدی که منجر به ریسک‌های امنیتی در بین شبکه‌های بی‌سیم در مقایسه با شبکه‌های کابلی می‌شوند:

کانال: شبکه‌های بی‌سیم معمولا درگیر ارتباطات رادیویی هستند، که بیشتر از شبکه‌های کابلی برای استراق سمع و پارازیت مستعد هستند.

پویایی: تجهیزات بی‌سیم، بطور قانونی و عموما در عمل بسیار قابل حمل‌تر و تحرک پذیرتر از تجهیزات کابلی هستند.

منابع: برخی تجهیزات بی‌سیم، همانند تلفن‌های هوشمند و تبلت‌ها، دارای سیستم عامل پیچیده‌ای هستند، اما حافظه و منابع پردازشی محدودی دارند و عموما با تهدیداتی چون حملات محرومیت – از - سرویس و بدافزارها روبرو می‌شوند.

قابلیت دسترسی: برخی از تجهیزات بی‌سیم، همانند سنسورها و ربات‌ها، ممکن است بدون متصدی و مراقب در محل‌هایی با دسترسی از راه دور/ یا مکانهای متعلق به مهاجمان باقی بمانند. این امر به شکل زیادی خطر حمله فیزیکی به آنها را افزایش می‌دهد.

تهدیدات امنیتی

در یک محیط بی‌سیم سه بخش امکان حمله را فراهم می‌کنند (تصویر زیر):

- یک کاربر بی‌سیم که می‌تواند یک تلفن بی‌سیم یا گوشی همراه، یک لپ‌تاپ یا تبلت دارای امکانات Wi-Fi، یک سنسور بی‌سیم و یا یک تجهیز مجهز به بلوتوث باشد.
- یک نقطه دسترسی بی‌سیم که یک اتصال به شبکه یا سرویس را فراهم می‌کند. مثالی از یک نقطه دسترسی همان برجهای سلولی، نقاط حساس Wi-Fiو نقطه دسترسی شبکه بی‌سیم به شبکه کابلی محلی یا گسترده است.
- بخش سوم همان رسانه انتقال، که امواج رادیویی را برای انتقال داده حمل می‌کند، است که خود منبع خطر نیز خواهد بود.

تهدیدهای شبکه بی سیم

ارتباط تصادفی: شبکه‌های بی‌سیم محلی یا نقطه دسترسی شبکه بی‌سیم به شبکه‌های محلی کابلی در مجاورت یکدیگر ممکن است همپوشانی در محدوده انتقال ایجاد نمایند.

انجمن مخرب: در این موقعیت، تنظیمات یک تجهیز بی‌سیم تغییر داده می‌شود تا یک نقطه دسترسی مجاز به نظر برسد، و عملگر را قادر می‌سازد تا رمزهای عبور را از یک کاربر مجاز دزدیده و سپس به یک شبکه کابلی از طریق یک نقطه دسترسی بی‌سیم نفوذ نماید.

شبکه‌های Ad-hoc :اینها شبکه‌های نقطه - به - نقطه بین کامپیوترهای بی‌سیم بدون وجود نقطه دسترسی مرکزی بین آنها هستند. این شبکه‌ها می‌توانند بسته به عدم وجود نقطه مرزی کنترلی در معرض تهدیدات امنیتی قرار گیرند.

شبکه‌های غیرسنتی: شبکه‌های غیرسنتی و لینک‌ها، همانند تجهیزات بلوتوث شبکه‌های شخصی، بارکد خوان‌ها، و کامپیوترهای کوچک قابل حمل همگی یک ریسک امنیتی در هر دو زمینه استراق سمع و دزدیدن اطلاعات خواهند داشت.

دزدیدن هویت (دزدیدن *MAC*): این اتفاق زمانی می‌افتد که یک مهاجم بتواند به ترافیک شبکه گوش داده و آدرس *MAC* کامپیوتر با مجوز شبکه را تشخیص دهد.

حملات مرد –در-میانه: این نوع حمله در فصل سوم در مفهوم پروتکل مبادله کلید دیفی - هیلمن بتفصیل شرح داده شده است.

حمله محرومیت از سرویس یا DOS: این مدل از حملات با جزییات در فصل دهم توضیح داده خواهد شد. در فضای شبکه‌های بی‌سیم از پروتکل مبادله کلید دیفی- هیلمن یک حمله DOS زمانی رخ می‌دهد که یک مهاجم به طور پیوسته یک نقطه دسترسی بی‌سیم یا برخی از گذرگاههای بی‌سیم در دسترس را با انواع پیام‌های طراحی شده برای مصرف منابع سیستمی بمباران نماید.

تزریق به شبکه یا Injection: یک حمله تزریق در واقع نقطه دسترسی شبکه بی‌سیم، که در معرض ترافیک فیلتر نشده مانند پیام پروتکل مسیریابی یا پیامهای مدیریت شبکه قرار دارد، را هدف قرار می‌دهد.

ایجاد امنیت در انتقالهای بی‌سیم

تهدیدات اصلی برای انتقال بی‌سیم شامل استراق سمع، دستکاری یا جایگزینی پیام، و درهم ریختن آن است. برای مقابله با استراق سمع و دستکاری و جایگزینی اطلاعات دو نوع راهکار مناسب وجود دارد:

تکنیکهای پنهان کردن سیگنال: سازمانها می‌توانند روشهایی را اتخاذ نمایند تا بتوانند این نوع حملات را برای یک مهاجم که بر روی نقطه دسترسی بی‌سیم واقع شده است، بسیار سخت‌تر نمایند، از آنجمله می‌توان به مواردی چون خاموش نمودن پخش همگانی شناسه مجموعه خدمات یا همان SSID بوسیله یک نقطه دسترسی بی‌سیم؛ اختصاص نامهای رمزی به SSIDها؛ کاهش سیگنالهای قوی به کمترین سطح که همچنان پوشش لازم را برای کاربران فراهم کنند؛ و قراردادن نقطه دسترسی بی‌سیم در داخل ساختمان، بدور از پنجره و دیوارهای خارجی اشاره نمود. امنیت بیشتر در این زمینه می‌تواند با استفاده از آنتن‌های جهت دار و تکنیک حفاظ - سیگنال حاصل شود.

رمزگذاری: رمزگذاری همه انتقالهای موجود در یک شبکه بی‌سیم در برابر حمله استراق سمع موثر خواهد بود البته تا جایی که کلیدهای رمزگذاری امن باشند. استفاده از رمزگذاری و پروتکل‌های احراز هویت روش استاندارد مقابله با تلاش‌های مهاجمان جهت دستکاری و جایگزینی اطلاعات در زمان انتقال است.

ایجاد امنیت در نقطه دسترسی بی‌سیم

1. از رمزگذاری استفاده کنید. مسیریابهای بی‌سیم معمولا با مکانیزم‌های رمزگذاری داخلی برای ترافیک موجود مسیریاب – به - مسیریاب تجهیز می‌شوند.

2. از نرم افزارهای آنتی ویروس، آنتی جاسوس افزارها و دیوارهای آتش استفاده کنید. این امکانات باید برروی همه نقاط پایانی شبکه‌های بی‌سیم فعال گردند.

3. پخش همگانی شناسه شبکه را غیر فعال نمایید. مسیریابهای بی‌سیم معمولا طوری تنظیم شده‌اند که یک سیگنال مشخص شده را پخش همگانی می‌نمایند، بنابراین هر تجهیزی در این محدوده می‌تواند در مورد موجودیت مسیریابها اطلاعاتی را بدست آورد. اگر یک شبکه تنظیم شود آنگاه تجهیزات مجاز می‌توانند شناسه مسیریابها را بدانند، این توانایی می‌تواند غیرفعال شود، بنابراین حملات مرتبط نیز خنثی خواهند شد.

4. شناسه مسیریاب را از حالت پیش فرض تغییر دهید. بازهم، این روش حملاتی که تلاش می‌کنند تا به شبکه بی‌سیم با استفاده از مشخصات پیش فرض مسیریابها دسترسی پیدا کنند را خنثی می‌نماید.

5. رمزعبور از پیش تنظیم شده مسیریاب برای راهبران شبکه را تغییر دهید. این یک گام محتاطانه دیگر خواهد بود.

6. فقط اجازه دهید کامپیوترهای مشخصی به شبکه بی‌سیم شما دسترسی پیدا کنند. یک مسیریاب می‌تواند به طریقی تنظیم شود که تنها با آدرس‌های MAC موافقت شده ارتباط برقرار نماید. البته، آدرس MAC می تواند جعل شود، و این فقط یک بخشی از استراتژی‌های امنیتی است.

نگرانی‌های عمده در مورد تجهیزات سیار

عدم کنترل امنیت فیزیکی: تجهیزات سیار معمولا تحت نظارت کامل کاربران بوده و در محل‌های مختلفی در خارج از کنترل سازمان مانند مکانهای خارج از ساختمان استفاده و نگهداری می‌شوند.

استفاده از تجهیزات سیار غیر قابل اطمینان: علاوه براین سازمانهایی که تجهیزات سیار را ارائه و کنترل می‌نمایند، بطور مجاز همه کارمندان دارای تلفن هوشمند و یا تبلت هستند.

استفاده از شبکه های غیر قابل اعتماد: اگر یک تجهیز سیار در محل استفاده شود، می‌تواند به منابع سازمان از طریق شبکه‌های بی‌سیم داخلی سازمان متصل شود.

استفاده از برنامه‌هایی که بوسیله افراد ناشناخته ایجاد شده اند: با طراحیهای امروزی، براحتی می‌توان برنامه‌های شخص سوم را بر روی تجهیزات سیار جستجو نموده و نصب کرد.

تعامل با دیگر سیستم‌ها: یک خصیصه مشترک در تلفن‌های هوشمند و تبلت‌ها توانایی همزمان سازی داده‌ها، برنامه‌های کاربردی، قراردادها، عکس‌ها، و موارد مشابه با تجهیزات کامپیوتری دیگر و امکانات ذخیره و بازیابی مبتنی بر محاسبات ابری است.

استفاده از محتویات غیرقابل اعتماد: تجهیزات سیار ممکن است به محتویاتی دسترسی پیدا نموده و از آنها استفاده کنند که سایر تجهیزات کامپیوتری نمی‌توانند از آنها بهره ببرند.

استفاده از سرویس‌های مکان‌یابی: توانایی GPS بر روی تجهیزات سیار می‌تواند برای نگهداری اطلاعات محل فیزیکی تجهیزات استفاده شود.

استراتژی امنیت

امنیت تجهیزات: چه تجهیز توسط سازمان ارائه شده باشد و چه مالکیت شخصی داشته باشد یعنی BYOD، باید سازمان تجهیز را با کنترل‌های امنیتی از جمله موارد زیر تنظیم نماید:

* فعال کردن قفل - خودکار، که باعث می‌شود تجهیز اگر مدت زمان تعیین شده‌ای استفاده نشود، قفل شده و کاربر می‌بایست یک شماره شناسایی شخصی 4 رقمی یا رمزعبور را دوباره وارد نماید تا تجهیز را فعال سازد.

* حفاظت از شماره شناسایی شخصی یا رمزعبور را فعال سازد. شماره شناسایی شخصی یا رمزعبور برای بازکردن قفل تجهیز لازم است. علاوه براین، می‌تواند پیکربندی نیز گردد، بنابراین آن پست الکترونیکی و داده‌های دیگر در تجهیز با استفاده از شماره شناسایی شخصی یا رمزعبور رمزنگاری می‌شود و فقط می‌تواند با همان شماره شناسایی شخصی یا رمزعبور دوباره بازیابی گردد.

* استفاده از ویژگی‌های کاملا خودکار که نام کاربر و کلمه عبور را به خاطر می‌سپارند اجتناب ورزد.

* توانایی کنترل از راه دور را از بین ببرد.

* اطمینان حاصل نماید که حفاظت SSL، در صورت موجود بودن، فعال شده باشد

* اطمینان حاصل نماید که نرم‌افزارها، از جمله سیستم عامل و برنامه‌های کاربردی، به روز شده باشند.

* نرم افزار آنتی ویروس، در صورت موجود بودن، نصب شده باشد.

داده‌های حساس باید از ذخیره شدن بر روی تجهیزات سیار منع شده یا اینکه رمزنگاری شوند.

* کارکنان فن‌آوری اطلاعات باید توانایی این را داشته باشند که از راه دور به تجهیزات سیار دسترسی داشته، دستگاه را از تمام داده‌ها پاک نموده، و سپس دستگاه را در صورت از دست رفتن یا سرقت، غیر فعال نماید.

استراتژی امنیت

* سازمان ممکن است تمام انواع نرم‌افزارهای شخص سوم را ممنوع نماید، یک لیست سفید برای ممنوعیت نصب تمام برنامه‌های تایید نشده تهیه نموده و یا یک sandbox امن پیاده‌سازی کند تا داده‌های سازمان را ایزوله نموده، برنامه‌های کاربردی را از سایر داده‌ها و برنامه‌های کاربردی روی تجهیزات سیار جدا نماید.

* سازمان می‌تواند محدودیت‌های مربوط به اینکه کدام تجهیزات می‌توانند از نظر زمانی بر هم منطبق بوده و از حافظه‌های مبتنی بر محاسبات ابری استفاده نمایند، را پیاده‌سازی و اجرا نماید.

* برای مقابله با خطرات مربوط به محتویات غیر قابل اعتماد، مسئولین برقراری امنیت می‌توانند مواردی چون ریسکهایی که از میان محتویات غیر قابل اعتماد انتشار خواهند یافت را آموزش دهند.

* برای مقابله با تهدیدات استفاده بد اندیشانه از سرویس‌های مکان‌یابی، سیاست‌های امنیتی می‌توانند امر کنند که این سرویس‌ها بر روی این تجهیزات سیار غیرفعال شوند.

امنیت ترافیک: امنیت انتقال اطلاعات مبتنی بر مکانیزم‌های استفاده شده برای رمزنگاری و احراز هویت می‌باشد. کل ترافیک باید رمزنگاری شده و بوسیله تجهیزات امن انتقال داده شوند، به عنوان مثال SSL و IPV6. همچنین شبکه‌های خصوصی مجازی یا همان VPN می‌توانند پیکربندی شوند و در نتیجه همه ترافیک بین تجهیزات سیار و شبکه سازمان می‌توانند از طریق یک VPN منتقل شوند.

یک پروتکل احراز هویت قوی باید استفاده شود تا دسترسی از تجهیزات را به منابع سازمان محدود نماید. در اغلب موارد، یک تجهیز سیار دارای یک تاییدکننده اعتبار اسناد مختص آن تجهیز می‌باشد، زیرا فرض بر این است که هر تجهیز تنها یک کاربر دارد. یک استراتژی برتر باید یک مکانیزم احراز هویت دو لایه داشته باشد، که ابتدا شامل احراز هویت تجهیز و سپس احراز هویت کاربر آن تجهیز نیز باشد.

معماری
IEEE 802.11

معماری

استانداردهای IEEE802.11در خلال معماری مجموعه‌ای از پروتکل‌های دارای لایه یا طبقه تعریف شده‌اند. این معماری، برای همه استانداردهای IEEE802.11 استفاده می‌شود، که شامل سه لایه است:

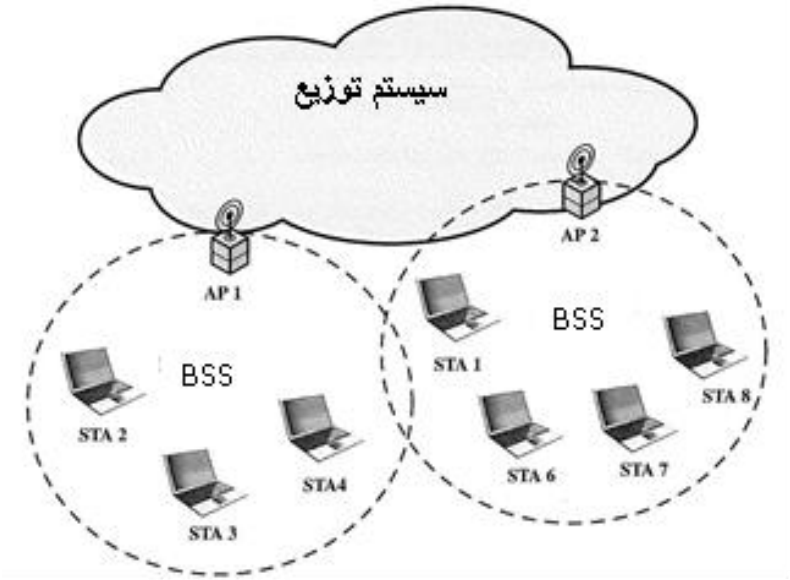
لایه فیزیکی: پایین‌ترین لایه از مدل مرجع IEEE802 لایه فیزیکی است، که در اصل شامل توابعی از قبیل رمزگذاری یا رمزگشایی سیگنالها و انتقال یا دریافت بیتهاست. علاوه بر آن، لایه فیزیکی شامل مشخصات رسانه انتقال نیز است. در مورد IEEE802.11 ، لایه فیزیکی همچنین باندهای فرکانس و ویژگی‌های آنتن را نیز تعریف می‌کند.

کنترل دسترسی به رسانه: تمامی شبکه‌های محلی شامل مجموعه‌ای از تجهیزاتی هستند که ظرفیت انتقال شبکه‌ها را به اشتراک می‌گذارند. در واقع لایه MAC داده را از پروتکل لایه بالاتر، معمولا از لایه کنترل لینک منطقی یا همان LLC، در قالب یک بلوکی از داده‌ها دریافت نموده و :

- در هنگام انتقال، داده‌ها را در یک قاب، به عنوان یک پروتکل واحد داده MAC یا MPDUبه همراه آدرس‌ها و فیلدهای کشف خطا سرهم می‌شوند.
- در دریافت، قاب را تجزیه نموده و عملیات شناسایی آدرس و تشخیص خطا انجام می‌گردد.
- دسترسی به رسانه انتقال شبکه را کنترل می‌نماید.

کنترل منطقی لینک: کشف خطاها با استفاده از CRC و اصلاح این خطاها با ارسال مجدد فریم-های آسیب برعهده این موجودیت است.

مدل معماری و اجزای شبکه IEEE 802.11



کوچکترین بلوک ساختمانی از شبکه‌های محلی بی‌سیم همان مجموعه پایه و اساسی خدمات یا BSS است، که شامل ایستگاه بی‌سیمی است که پروتکل MAC مشابه را اجرا نموده و برای دسترسی به رسانه بی‌سیم مشترک رقابت می‌کند. یک BSS ممکن است جدا باشد و یا ممکن است به یک سیستم اصلی پخش یا DS از طریق نقطه دسترسی یا همان AP متصل شود. در اینجا AP همانند پل و نقطه پاسخ عمل می‌کند. در BSS ایستگاههای مشتری به طور مستقیم با یکدیگر ارتباط برقرار نمی‌کنند. ترجیحا، اگر یک ایستگاه در BSS بخواهد با ایستگاه دیگری در BSS مشابه تماس برقرار کند، ابتدا آدرس قالبMAC از ایستگاه اصلی به AP فرستاده می‌شود و سپس از AP به ایستگاه مقصد ارسال می‌گردد.

زمانی که همه ایستگاهها در BSS همان ایستگاههای سیار هستند و به طور مستقیم با هم ارتباط برقرار می‌کنند (یعنی از AP استفاده نمی‌کنند)، آنگاه BSS یک BSS مستقل یا در اصطلاح IBSS نامیده می‌شود.

توزیع پیام در یک سیستم توزیع یا DS

دو سرویسی که در توزیع پیام درون یک DS دخالت دارند عبارتند از توزیع و یکپارچگی. توزیع یک سرویس اولیه است که توسط ایستگاه استفاده می‌شود تا مبادلات را انجام دهد. بخصوص زمانی که داده ها باید از یک ایستگاه در یک BSS به یک ایستگاه در یکی ازBSSهای دیگر عبور کند.

برای مثال، فرض کنید یک قاب موجود از ایستگاه دوم (STA2) به ایستگاه هفتم (STA7) در تصویر صفحه قبل فرستاده می‌شود. قاب از STA2به AP1، که AP مربوط به این BSS است، فرستاده می شود. آنگاه AP این قاب را به DS می‌فرستد، که وظیفه دارد تا قاب را به APمرتبط با STA7 در BSS هدف بفرستد. حال AP2، قاب را دریافت نموده و آنرا رو به جلو به ایستگاه هفتم می‌فرستد. اینکه چگونه پیام از طریق DS انتقال یافته است فراتر از محدوده استانداردIEEE 802.11 خواهد بود.

اگر دو ایستگاه که در حال برقراری ارتباط هستند درون یک BSS مشابه باشند، آنگاه سرویس توزیع منطقی از طریق یک AP واحد درون BSS عبور داده می‌شود.

پویایی یا سیار بودن

قبل از اینکه به دنبال مفهوم ارتباط باشیم، نیاز به توصیف مفهوم پویایی یا سیاربودن داریم.
استاندارد سه نوع انتقال، را بر اساس سیاربودن تعریف می‌کند:

انتقال ثابت: ایستگاه از این نوع یا ثابت است و یا تنها در محدوده‌ای که بتواند ارتباط مستقیم با ایستگاه‌های یک BSS برقرارکند، حرکت می‌کند.

انتقال BSS: این نوع برای مواردی که یک ایستگاه از یک BSS به BSS دیگر در داخل همان ESS تعریف شده، حرکت نماید، تعریف شده است. در این مورد، عملیات تحویل داده‌ها به ایستگاه نیازمند آن است که قابلیت آدرس دهی قادر به تشخیص محل جدید ایستگاه باشد.

انتقال ESS: این نوع برای مواردی که یک ایستگاه از BSS در یک ESS به یک BSS درون ESS دیگر حرکت نماید، تعریف شده است. این مورد تنها در زمانی حمایت می‌شود که ایستگاه بتواند جابجا شود. البته در اینجا نگهداری از ارتباطات لایه بالاتر که توسط 802.11 پشتیانی می‌شود، تضمین نخواهد شد. در واقع، اختلال در ارائه خدمات به احتمال زیاد رخ خواهد داد.

پس برای انتقال یک پیام در یک DS چه باید کرد؟

سرویسهای انتقال پیام

برای انتقال یک پیام در یک DS، سرویس توزیع نیازمند آن است که محل ایستگاه مقصد را بداند. به طور خاص،DS نیاز به دانستن هویت آن AP که پیام باید به آن منتقل شود، دارد تا پیام به ایستگاه مقصد برسد. برای برآورده کردن این نیاز، یک ایستگاه باید ارتباطش را با AP در درون BSS فعلی حفظ کند.

سه سرویس مربوط به این نیاز عبارتند از:

* **ارتباط:** یک ارتباط اولیه بین یک ایستگاه و AP ایجاد می‌کند. پیش از اینکه ایستگاه بتواند بسته‌ها را بر روی یک شبکه محلی بی‌سیم انتقال دهد یا دریافت نماید، موجودیت و آدرسش باید شناخته شود. برای این منظور، یک ایستگاه باید یک ارتباط با یکAP درون یک BSS خاص برقرار سازد. AP می‌تواند این اطلاعات را با APهای دیگر درون ESS مراوده نماید تا مسیریابی و تحویل بسته مورد خطاب را تسهیل نماید.

* **ارتباط مجدد:** یک ارتباط برقرار شده را قادر می‌سازد تا از یک AP به AP دیگر منتقل شود، همچنین اجازه می‌دهد یک ایستگاه سیار از یک BSS به BSS دیگر حرکت کند.

* **پایان ارتباط**: یک پیغام از یک ایستگاه یا یک AP که بیان می‌کند، ارتباط قطع شده است. ایستگاه باید این اطلاع رسانی را پیش از ترک ESS یا بستن ارتباط انجام دهد. با این حال، مرکز مدیریت MAC خود را در برابر ایستگاههایی که بدون اطلاع ناپدید می‌شوند، محافظت خواهد کرد.

امنیت شبکه های محلی بی سیم

ویژگی های اصلی

دو ویژگی در شبکه‌های محلی کابلی وجود دارند که به شبکه‌های محلی بی‌سیم به ارث نمیرسند:

1. برای انتقال در شبکه‌های کابلی محلی، یک ایستگاه باید به شکل فیزیکی به شبکه محلی متصل شود. در حالی که، در یک شبکه محلی بی‌سیم، هر ایستگاه درون محدوده رادیویی سایر تجهیزات درون شبکه محلی، می‌تواند عملیات انتقال را انجام دهد. این بدان معنی است که، در اینجا یک فرم خاصی برای احراز هویت بوسیله یک شبکه کابلی وجود دارد که بر پایه تعدادی عملکرد مثبت و احتمالا یک سری از عملیات قابل مشاهده برای اتصال یک ایستگاه به یک شبکه محلی کابلی پایه‌ریزی شده است.

2. به طور مشابه، به منظور دریافت یک عملیات انتقال از یک ایستگاه که یک بخشی از شبکه محلی کابلی است، ایستگاه دریافت کننده نیز باید به یک شبکه محلی کابلی متصل شود. در حالی که، در شبکه‌های بی‌سیم، هر ایستگاه درون محدوده رادیویی می‌تواند اطلاعات را دریافت نماید. بنابراین، یک شبکه محلی کابلی یک درجه از حفظ حریم خصوصی کاربران را فراهم می‌نماید، که در واقع دریافت داده را فقط به ایستگاههای متصل به شبکه محلی محدود می‌سازد.

این تفاوتها بین شبکه‌های محلی کابلی و بی‌سیم افزایش نیاز به سرویس‌ها و مکانیزمهای امنیتی قوی برای شبکه‌های محلی بی‌سیم را نشان می‌دهد.

خدمات امنیتی

مجموعه امنیتی RSN مربوط به 802.11i خدمات زیر را تعریف می‌کند:

* **احراز هویت:** یک پروتکل که برای تعریف مبادله بین یک کاربر و یک AS استفاده می‌شود تا تصدیق دوجانبه را فراهم نموده و کلیدهای موقتی را تولید نماید که بر روی اتصالهای بی‌سیم بین کاربر و AP استفاده شوند.

* **کنترل دسترسی:** این تابع استفاده از تابع احراز هویت را تاکید می‌کند، پیام به درستی مسیریابی می‌شود، و مبادله کلید را تسهیل می‌نماید. این تابع می‌تواند با انواع مختلف از پروتکل‌های احراز هویت همکاری نماید.

* **حفظ حریم خصوصی با یکپارچگی پیام:** داده‌های در سطح MAC همراه با یک کد یکپارچگی پیام رمزگذاری می‌شوند که تضمین می‌کنند، داده‌ها تغییر نمی‌کنند.

مراحل عملیاتی این خدمات چگونه است؟

پیش فرض ها و مراحل عملیاتی

مراحل عملیاتی در استادارد IEEE 802.11i می‌تواند به 5 مرحله متمایز تقسیم شود (تصویر صفحه بعد). ماهیت واقعی این مراحل به پیکر بندی و نقاط پایانی ارتباطات بستگی دارد. فرضیات شامل موارد زیر خواهند بود :

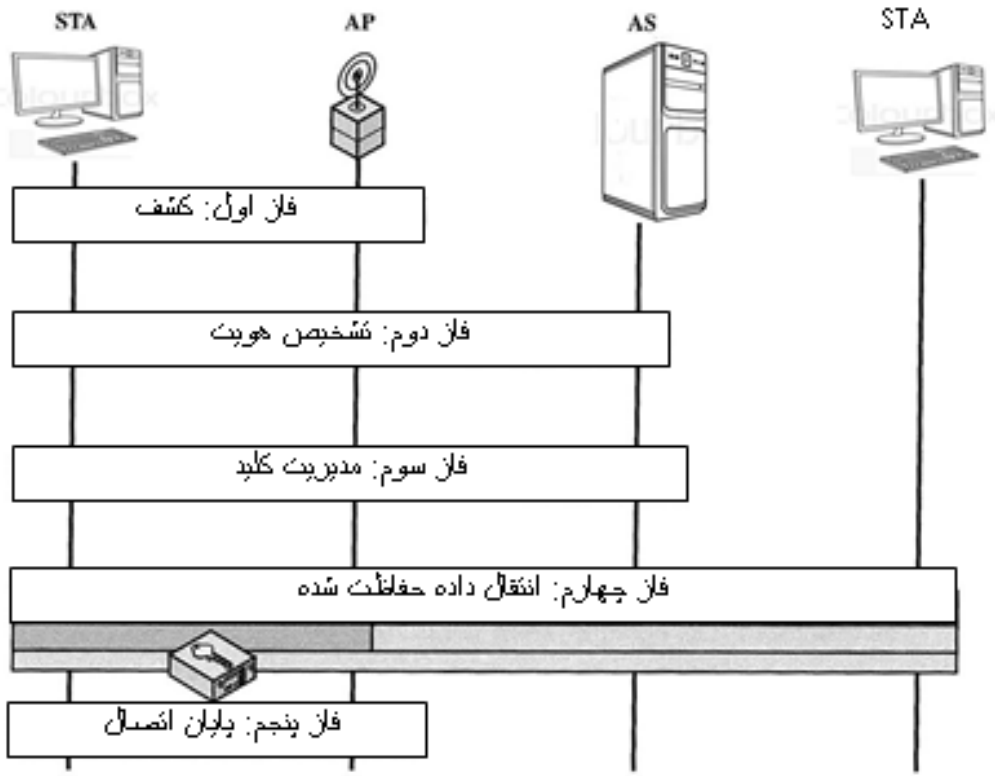
1. دو ایستگاه بی‌سیم در یک BSS مشابه که از طریق یک AP موجود در آن BSS با هم ارتباط برقرار می‌کنند.

2. دو ایستگاه بی‌سیم یا STA در یک شبکه adhoc یکسان بطور مستقیم با یکدیگر ارتباط دارند.

3. دو ایستگاه بی‌سیم درBSSهای متفاوت از طریقAPهای مربوطه از میان یک سیستم توزیع، ارتباط برقرار می‌کنند.

4. یک ایستگاه بی‌سیم، با یک ایستگاه پایانی روی یک شبکه کابلی، از طریق AP و سیستم توزیع ارتباط برقرار می‌کند.

پیش فرض ها و مراحل عملیاتی



پیش فرض ها و مراحل عملیاتی

* **کشف:** یک APاز پیامهایی به نام Beacons و Probe استفاده می‌کند تا سیاست‌های امنیتی IEEE 802.11i را اعمال نماید. در اصل STAاز این امر برای شناسایی APمربوط به شبکه محلی بی‌سیم که مایل به برقراری ارتباط با آن است، استفاده می‌کند. در واقع اینجا STA با AP ارتباط برقرار می‌کند، تا روش‌های احراز هویت و روش‌های مدیریت کلیدهای رمزنگاری را برگزینند.

* **تایید:** در این مرحله، STA و AS هویتشان را به یکدیگر ثابت می‌کنند. بلوک‌های AP ترافیک احراز هویت نشده بین STAو AS را تا زمانی که عملیات احراز هویت موفق شود، مسدود خواهند کرد. در اصل AP در عملیات احراز هویت به غیر از بخش انتقال ترافیک مابین STA و AS شرکت نمی‌کند.

* **تولید و توزیع کلید:** در اصل AP و STA عملیات بسیاری را اجرا می‌کنند که نیازمند تولید کلید رمزنگاری و ذخیره شدن در AP و STA هستند. فریم‌ها فقط بین AP و STA جابه‌جا می‌شوند.

* **انتقال داده حفاظت شده:** فریم‌ها بین STA و ایستگاه پایانی درون AP مبادله می‌شوند. همانطور که براساس مدلهای رمزنگاری تعریف شده است، در اینجا امنیت تنها بین STA و AP اعمال می‌شود و در واقع امنیت انتها - به - انتها فراهم نمی‌گردد.

* **خاتمه ارتباط:** در اصل AP و STA فریم‌ها را مبادله کرده‌اند. در این مرحله، اتصال امن به پایان رسیده و اتصال به حالت اولیه بازگردانده می‌شود.

سوالات مرتبط

1. بلوک پایه شبکه بی‌سیم 802.11 چیست؟
2. یک مجموعه سرویس تعمیم یافته را تعریف نمایید؟
3. سرویسهای IEEE 802.11 را نام برده و بطور مختصر شرح دهید؟
4. آیا یک شبکه بی سیم یک سیستم توزیع شده است؟
5. چه بخشهایی از امنیت در استاندارد IEEE 802.11i در نظر گرفته شده است؟
6. بطور خلاصه پنج فاز عملیاتی استاندارد IEEE 802.11i را شرح دهید؟

خلاصه: امنیت بی‌سیم، تهدیدهای شبکه بی سیم، ایجاد امنیت در انتقالهای بی‌سیم، نگرانی‌های عمده در مورد تجهیزات سیار ، استراتژی امنیت، مدل معماری و اجزای شبکه IEEE 802.1، خدمات امنیتی

جلسه بعدی: امنیت IP

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

ترجمه: دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.