نقاط دسترسی غیرمجاز و حمله‌ی مردی در میانه در شبکه‌های محلی بی‌سیم 802.11

فرهود فریداعتماد

fa.faridetemad@gmail.com

آزمایشگاه تخصصی آپا در زمینه امنیت فن‌آوری اطلاعات و ارتباطات

http://cert.um.ac.ir

cert@um.ac.ir

ویرایش اول – خردادماه ۱۳۹۳

شماره سند: APA_FUM_W_WiFi_0118

چکیده

از تهدیدات جدی در شبکه‌های محلی بی‌سیم، به‌کارگیری نقاط دسترسی بی‌سیم غیرمجاز در شبکه است که زمینه‌ساز دسترسی غیرمجاز به زیرساخت کابلی شبکه یا انجام حملات نظیربه‌نظیر بر روی سیستم‌های مشتریان می‌گردد. این مقاله به تحلیل و بررسی این دو تهدید در غالب دو عنوان "دستگاه‌های بی‌سیم غیرمجاز داخلی" و "حمله‌ی مردی در میانه (MitM) می‌پردازد. آشنایی با این دو تهدید، خسارت‌های ناشی از آن‌ها و روش‌های مقابله در جهت تامین امنیت شبکه‌های محلی بی‌سیم برای کاربران و مدیران شبکه‌های بی‌سیم ضروری است.

واژه‌های کلیدی

دسترسی غیرمجاز، تهدید، حمله‌ی مردی در میانه، MitM، Evil twin، Rogue Access Point، 802.1X/EAP.

۱- مقدمه

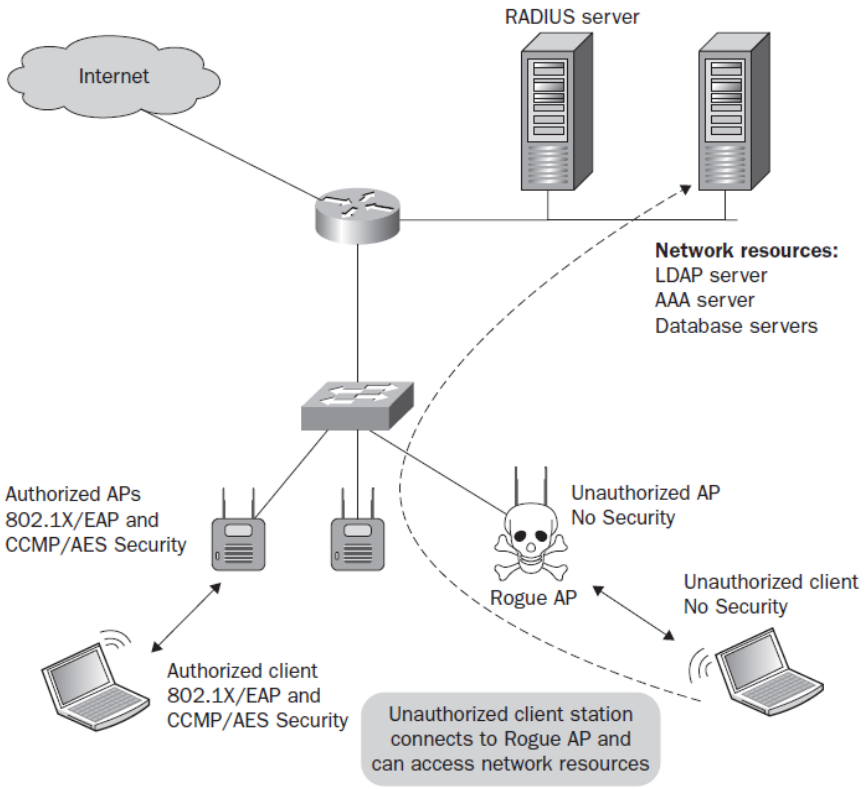
همواره وجود *نقاط دسترسی مخرب*[1] در شبکه‌های محلی بی‌سیم از برجسته‌ترین تهدیدهای این حوزه تلقی گردیده است. با در نظر گرفتن شبکه‌های محلی بی‌سیم به عنوان درگاهی مجاز به سوی منابع شبکه‌ی سازمان، اشخاصی ممکن است تلاش کنند درگاه اختصاصی خود را برای دسترسی به منابع بر روی زیرساخت شبکه برپا کنند. این‌جا نقطه‌ای است که تهدید دستگاه‌های بی‌سیم غیرمجاز و به خصوص نقاط دسترسی مخرب مطرح می‌گردد. از آن‌جا که استفاده‌ی غیرمجاز نقاط دسترسی بی‌سیم شایع‌تر از سایر دستگاه‌های بی‌سیم است، عنوان "نقطه‌ی دسترسی مخرب" غالبا به جای "دستگاه بی‌سیم مخرب" استفاده می‌شود.

در مبحث دسترسی غیرمجاز در شبکه‌های محلی بی‌سیم، نقاط دسترسی مخرب را می‌توان در دو گروه طبقه‌بندی کرد. نقطه‌ی دسترسی غیرمجاز داخلی، که عموما توسط عاملی داخلی مانند کارمند شرکت و به منظور تسهیل استفاده از شبکه به زیرساخت شبکه متصل و استفاده می‌شود. در این صورت، کارمند به طور ناخواسته درگاهی به زیرساخت شبکه راه‌اندازی کرده که خارج از نظارت و فاقد کنترل‌های امنیتی لازم است. تهدید مربوط به این نوع دسترسی غیرمجاز در بخش ۲ مقاله‌ی حاضر تشریح می‌گردد. نوع دیگر که شناسایی و کنترل آن دشوارتر است، شامل مواردی است که مهاجم با برپایی و کنترل نقطه‌ی دسترسی مخربی که مشابه نقطه‌ی دسترسی مجاز به نظر می‌آید، اتصال کاربران شبکه‌ی بی‌سیم را از نقطه‌ی دسترسی مجاز می‌رباید. در نتیجه، ترافیک قربانی کاملا از ماشین مهاجم عبور کرده و زمینه‌ی انجام حملات مردی در میانه (MitM[2]) را فراهم می‌نماید. استفاده از این نوع نقطه‌ی دسترسی مخرب و تهدیدهای ایجاد شده در پی آن، در حال حاضر از برجسته‌ترین تهدیدها در شبکه‌های محلی بی‌سیم به شمار می‌رود. بحث مربوط به حمله‌ی مردی در میانه در شبکه‌های محلی بی‌سیم در بخش سوم از مقاله خواهد آمد.

[1] Rogue access points
[2] Man-in-the-Middle attacks

۲- دستگاه‌های بی‌سیم غیرمجاز داخلی

در یک سازمان ممکن است یک یا چند شبکه‌ی بی‌سیم به طور خودسر راه‌اندازی شده باشند، در حالی که مسؤولان سازمان از آن بی‌اطلاع هستند. افراد، مسؤول برپایی نقطه‌ی دسترسی بی‌سیم هکرها نیستند؛ بلکه معمولا این کارمندان داخلی سازمان هستند که اقدام به راه‌اندازی شبکه‌ی بی‌سیم اختصاصی خود می‌نمایند. این افراد که به استفاده از شبکه‌ی بی‌سیم عادت کرده‌اند، برای سهولت در استفاده از شبکه اقدام به اتصال نقطه‌ی دسترسی بی‌سیم به شبکه‌ی کابلی سازمان نموده و ناآگاهانه سازمان خود را در معرض ریسک قرار می‌دهند. طبق تعریف [۱]، هر دستگاه مجهز به رادیو که به طور غیرمجاز به زیرساخت کابلی شبکه متصل بوده و خارج از قلمرو مدیریتی ناظران شبکه قرار گیرد، یک دستگاه بی‌سیم مخرب است. بر این اساس، یک دستگاه بی‌سیم مخرب می‌تواند شامل نقطه‌ی دسترسی، پرینتر بی‌سیم و دوربین‌های بی‌سیم گردد. تهدید از آن‌جا سرچشمه می‌گیرد که این نقاط دسترسی ممکن است دسترسی به شبکه برای کارمندان را تسهیل نمایند، اما اکثرا ناامن هستند.



شکل (۱) : دسترسی غیرمجاز بی‌سیم به کمک نقطه‌ی دسترسی مخرب داخلی

هر نقطه‌ی دسترسی بی‌سیم خانگی می‌تواند به یک درگاه فعال اترنت (نقطه‌ی دسترسی شبکه) متصل شده و تبدیل به یک نقطه‌ی دسترسی مخرب بی‌سیم گردد. نقطه‌ی دسترسی مخرب، یک دروازه‌ی دسترسی بالقوه به زیرساخت کابلی سازمان است که هر شرکتی تمایل به محافظت از آن دارد. شکل (۱) این واقعیت را به تصویر کشیده است.

۲-۱- عوامل تهدید در دسترسی غیرمجاز داخلی

مواردی مشاهده شده که در برخی صنایع و ساختارهای دولتی به منظور جاسوسی یا سایر اهداف بدخواهانه، مهاجمان به طور خاص از نقطه‌ی دسترسی بی‌سیم مخرب استفاده کرده‌اند. با این حال، اکثر دستگاه‌های بی‌سیم مخرب با اهداف بدخواهانه به کار گرفته نمی‌شوند [1]. اغلب دستگاه‌های بی‌سیم مخرب توسط کاربران مجاز شبکه، کارمندان یا بازدیدکنندگان از سازمان در شبکه‌ی سازمان قرار می‌گیرند. این دسته از افراد دارای حق دسترسی روزانه به محوطه‌ی فیزیکی داخل سازمان هستند، امتیازی که یک مهاجم خارجی با هدف بدخواهانه از آن بی‌بهره است. این اشخاص مورد اعتماد به ندرت نقطه‌ی دسترسی مخرب را برای مقاصد بدخواهانه به کار می‌گیرند. انگیزه‌ی آن‌ها از به‌کارگیری این نقاط دسترسی بی‌سیم، افزایش برد عملیاتی بی‌سیم یا گسترش آن به نقاطی است که به عقیده‌ی آن‌ها باید دارای پوشش بی‌سیم باشد (بدون اخذ مجوزهای سازمانی). به دلیل فقدان سیاست امنیتی و آگاهی‌رسانی مناسب در خصوص دستگاه‌های بی‌سیم، گاهی اوقات این افراد داخلی سازمان نمی‌دانند که عملی اشتباه و زیان‌بار انجام می‌دهند.

گروهی دیگر از عاملان داخلی این تهدید، افرادی هستند که آگاهی دارند عمل‌شان برخلاف سیاست امنیتی سازمان است. با این حال، نیاز خود به استفاده از شبکه‌ی بی‌سیم را بر نقض سیاست امنیتی سازمان مقدّم می‌دانند. این گروه غالبا سعی می‌کنند دستگاه غیرمجاز خود را در مکانی مانند زیر میز و یا سایر جاهای دیگر مخفی کنند. در مواردی، دستگاه‌های غیرمجاز حتی در اتاق‌های سرور نیز کشف شده‌اند که توسط پرسنل فن‌آوری اطلاعات و برخلاف سیاست امنیتی سازمان مورد استفاده قرار می‌گرفتند.

با وجود این که تنها یک نقطه‌ی دسترسی ناامن جهت ورود غیرمجاز به شبکه و دسترسی به منابع سازمان کافی است، مواردی مشاهده گردیده است که در یک سازمان ده‌ها دستگاه بی‌سیم غیرمجاز کشف گردیده است. اغلب این دستگاه‌ها حتی مسیریاب‌های بی‌سیم خانگی 802.11 بوده و با قیمتی ارزان‌تر از یک نقطه‌ی دسترسی بی‌سیم به راحتی قابل تهیه هستند. یک کمپانی ارایه‌دهنده‌ی خدمات بی‌سیم در آمریکا به نام Netrepid در سال ۲۰۰۷ میلادی

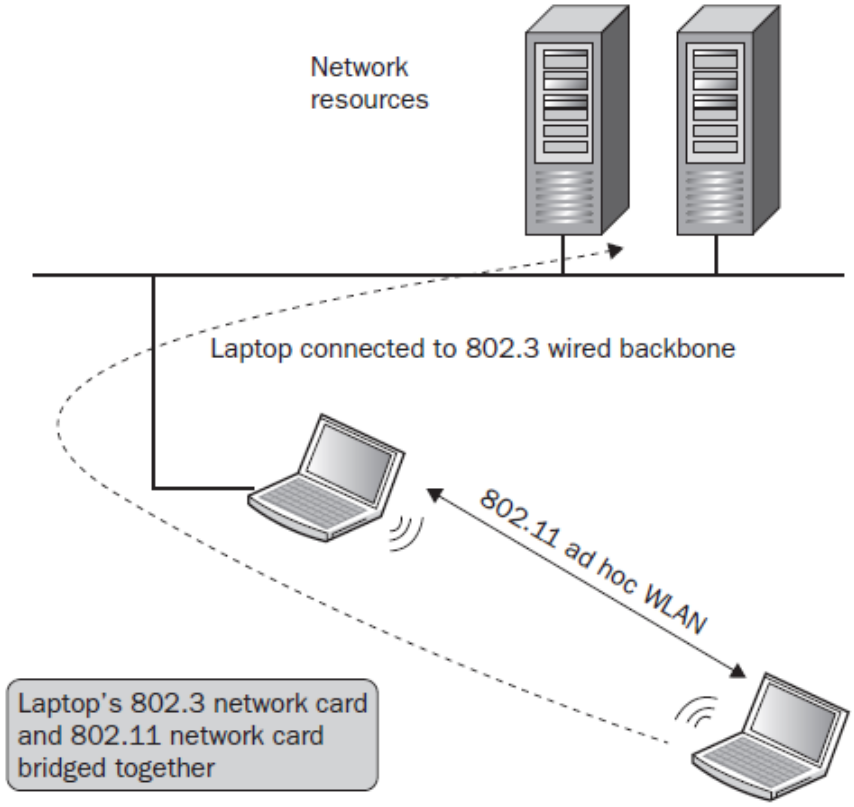
پس از بررسی که روی یک بیمارستان انجام داد، ۷۵ نقطه‌ی دسترسی غیرمجاز را در ساختمان اصلی آن کشف کرد. این در حالی است که پیش از بررسی، واحد فن‌آوری اطلاعات بیمارستان باور داشت هیچ دستگاه بی‌سیم غیرمجازی در ساختمان وجود ندارد. اکثر این نقاط دسترسی مسیریاب‌های بی‌سیم خانگی بودند [1].

۲-۲- انواع دستگاه‌های بی‌سیم غیرمجاز

در این بخش از مقاله، دستگاه‌های گوناگون بی‌سیم که قابلیت به‌کارگرفته شدن در دسترسی غیرمجاز به شبکه‌ی بی‌سیم را دارند، شرح داده می‌شوند. نقطه‌ی دسترسی بی‌سیم، ایستگاه‌های ad hoc، چاپگرها و دوربین‌های بی‌سیم در این زمره قرار می‌گیرند که در ادامه به بررسی آن‌ها پرداخته می‌شود.

یکی از شایع‌ترین شبکه‌های آسیب‌پذیر که کمتر مورد توجه قرار می‌گیرد، شبکه‌ی بی‌سیم ad hoc است. در اصطلاح فنی، شبکه‌ی محلی بی‌سیم 802.11 با توپولوژی ad hoc را IBSS[1] می‌نامند. شایان ذکر است دستگاه‌هایی که درون یک IBSS با هم ارتباط برقرار می‌کنند، صرفا شامل ایستگاه‌های مشتری بوده و در این ساختار نقطه‌ی دسترسی مرکزی وجود ندارد. به این ترتیب، یک IBSS شامل دو یا چند ایستگاه مشتری است که در محدوده‌ی فیزیکی مجاور هم به صورت نظیر به نظیر با یکدیگر شبکه شده‌اند. متاسفانه، شبکه‌های ad hoc دارای این آسیب‌پذیری هستند که منابع شبکه را در معرض دسترسی غیرمجاز قرار دهند. اغلب اتفاق می‌افتد که یک کارمند لپ‌تاپ یا رایانه‌ی رومیزی خود را از طریق کابل اترنت به شبکه‌ی سازمان متصل نموده است (اتصال 802.3). همین کارمند به طور همزمان از طریق کارت واسط بی‌سیم خود، یک شبکه‌ی ad hoc را در اتصال با رایانه‌ی یک کارمند دیگر برپا کرده است. اترنت و کارت بی‌سیم متعلق به یک سیستم می‌توانند به هم پل[2] شوند. در این صورت، یک مهاجم می‌تواند با اتصال به شبکه‌ی ad hoc، از طریق اتصال اترنت به زیرساخت کابلی سازمان نیز دسترسی پیدا کند. این سناریو در شکل ۲ به نمایش در آمده است.

[1] Independent Basic Service Set
[2] Bridge



شکل (۲): شبکه‌ی ad hoc پل شده به اترنت

نوعی دیگر از دستگاه‌های بی‌سیم مخرب نوظهور، چاپگرهای بی‌سیم هستند. بسیاری از چاپگرهای امروزی دارای رادیوی 802.11 هستند و از مد ad hoc نیز پشتیبانی می‌کنند. سناریوی منجر به دسترسی غیرمجاز برای این دستگاه‌ها به این ترتیب است که ابتدا مهاجم از طریق ابزار مدیریتی دستگاه که توسط کمپانی سازنده ارایه شده به چاپگر متصل می‌شود. این ابزار معمولا دارای واسط کاربری تحت وب بوده و یا از سایت کمپانی سازنده به راحتی قابل دانلود است. به کمک این ابزار مدیریتی، مهاجم می‌تواند Firmware دلخواه خود را روی چاپگر بارگذاری نموده و بدین ترتیب قادر خواهد بود اتصال بی‌سیم و اترنت چاپگر را پل نماید. در نتیجه، مهاجم می‌تواند حتی بدون استفاده از نقطه‌ی دسترسی بی‌سیم مخرب به شبکه‌ی کابلی سازمان دسترسی یابد. این رخنه‌ی امنیتی در بسیاری از دوربین‌های نظارت تصویری بی‌سیم نیز دیده می‌شود.

۲-۳- خسارت‌های ناشی از دستگاه‌های بی‌سیم مخرب داخلی

تهدید دستگاه‌های بی‌سیم مخرب داخلی، سبب رخنه در مکانیزم کنترل دسترسی برای منابع شبکه‌ی سازمان می‌گردد. در معرض دسترسی قرار گرفتن منابع شبکه، ریسک‌ها و خسارت‌های زیر را در پی خواهد داشت:

- **سرقت داده‌ها:** داده‌های قرار گرفته بر روی سرویس‌دهنده‌های پایگاه داده‌ها به مخاطره می‌افتند. داده‌هایی شامل اطلاعات حساب‌های بانکی، کارت‌های اعتباری، اسناد محرمانه‌ی تجاری، اطلاعات پرسنل و داده‌های پزشکی در صورتی که از طریق یک دستگاه مخرب در دسترس قرار گیرند، می‌توانند به سرقت روند. داده‌هایی که روی سرویس‌دهنده‌های شبکه یا کامپیوترهای رومیزی سازمان قرار گرفته‌اند، تماما در معرض ریسک خواهند بود. سرقت اطلاعات غالبا شایع‌ترین ریسک مرتبط با به‌کارگیری دستگاه‌های بی‌سیم مخرب است.
- **نابودی داده‌ها:** به طور مشابه، از بین رفتن داده‌ها نیز ممکن است رخ دهد. به این ترتیب که پایگاه‌های داده‌ها پاک گردیده و درایوها فرمت شوند.
- **از کار افتادن سرویس‌های شبکه:** حتی در صورتی که داده‌ای از بین نرود، مهاجم می‌تواند از طریق نقطه‌ی دسترسی مخرب، سرویس‌های شبکه را از کار بیاندازد. قطع یک یا چند سرویس مانند پست الکترونیکی منجر به کاهش بازدهی گردیده و برای یک سازمان خسارات قابل توجهی را در پی خواهد داشت.
- **جاسازی داده‌های مخرب:** یک مهاجم می‌تواند با استفاده از یک درگاه غیرمجاز اقدام به قرار دادن بدافزار و محتویات غیرقانونی بر روی شبکه نماید. برنامه‌های کنترل شونده‌ی از راه دور و جاسوسی مانند ثبت کننده‌های کلید از جمله برنامه‌هایی هستند که مهاجم می‌تواند با قرار دادن آن‌ها در شبکه به جمع‌آوری اطلاعات بپردازد. قرار دادن نرم‌افزارها و محتویات غیرمجاز بر روی سرویس‌دهنده‌ی FTP شبکه به منظور توزیع غیرقانونی نرم‌افزار، از دیگر موارد مشاهده شده است.
- **حملات به سایر شبکه‌ها:** با آسیب‌پذیر شدن شبکه از طریق دسترسی غیرمجاز بی‌سیم، زیرساخت شبکه‌ی قربانی می‌تواند به عنوان عاملی برای راه‌اندازی حمله به سایر شبکه‌ها در سراسر اینترنت تبدیل شود. مهاجم با کنترل شبکه‌ی قربانی می‌تواند اقدام به راه‌اندازی حملات *جلوگیری از سرویس توزیعی*[1] نماید. هر چه وسعت منابع و زیرساخت شبکه‌ی عامل حمله بیشتر باشد، خسارات ناشی بر روی شبکه‌ی هدف بیشتر خواهد بود.

[1] Distributed Denial os Service (DDoS)

فرستندگان هرزنامه از مدت‌ها پیش دریافته‌اند که می‌توانند از یک نقطه‌ی دسترسی بی‌سیم مخرب برای ارسال هرزنامه استفاه کنند.

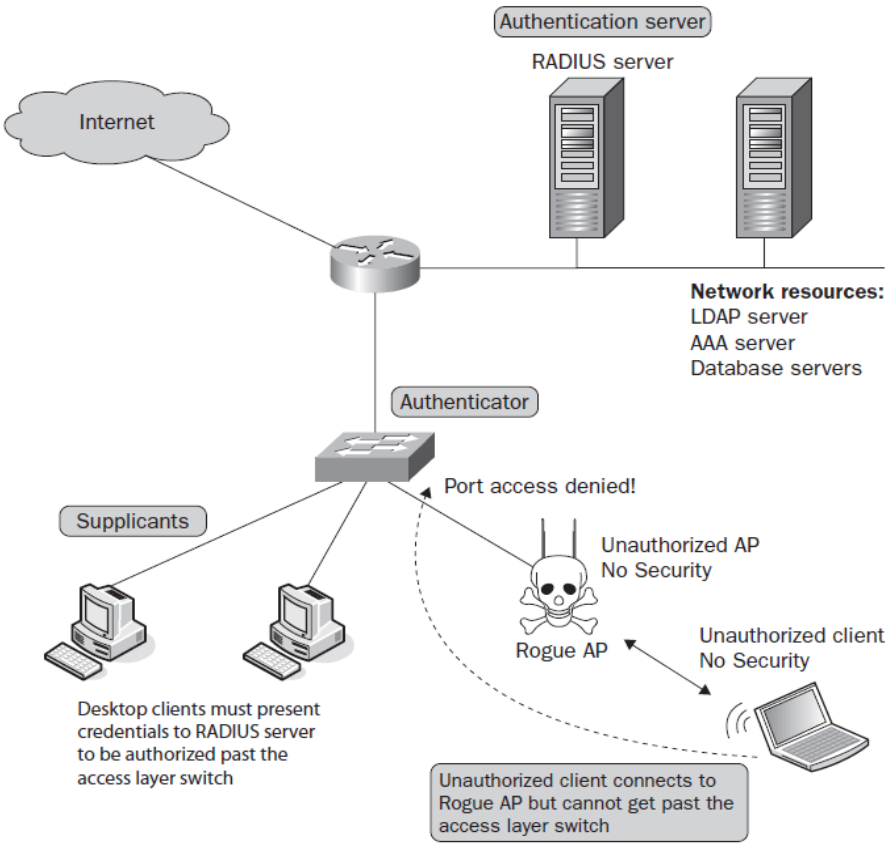
۲-۴- مقابله با نقاط دسترسی غیرمجاز داخلی

در این بخش از مقاله به توضیح راه‌های پیشگیری و مقابله با تهدید دستگاه‌های بی‌سیم داخلی پرداخته می‌شود. سیاست امنیتی سازمانی مناسب همراه با آگاهی‌رسانی، به کارگیری *سیستم‌های تشخیص/جلوگیری از نفوذ بی‌سیم*[1] و کنترل دسترسی مبتنی بر پورت از راهکارهای مقابله‌ای هستند که در ادامه توضیح داده خواهند شد.

از اقدامات اولیه برای پیشگیری از تهدید دستگاه‌های مخرب بی‌سیم، منع استفاده از نقاط دسترسی بی‌سیم غیرمجاز توسط پرسنل است. این موضوع باید در سیاست امنیتی سازمان صریحا ابلاغ گردد. همچنین، اکثر سازمان‌ها استفاده از شبکه‌های ad hoc را نیز ممنوع می‌کنند. برای این منظور، قابلیت شبکه‌سازی ad hoc در سیستم‌های مشتریان سازمان می‌تواند غیرفعال گردد. همچنین، قابلیت پل زدن بین کارت واسط بی‌سیم 802.11 و واسط اترنت 802.3 در ماشین‌های مشتری بی‌سیم می‌تواند غیرفعال شود. این کار با به‌کارگیری نرم‌افزارهای امنیتی بر روی ماشین‌های کاربران قابل انجام است. اعمال سیاست امنیتی و آگاهی‌رسانی، نقطه‌ی شروع مناسبی برای مقابله با خطر دستگاه‌های بی‌سیم مخرب است، اما با این حال نمی‌تواند مانع قطعی استفاده از نقطه‌ی دسترسی بی‌سیم شخصی توسط افراد دارای انگیزه گردد.

مؤثرترین روش برای مقابله با تهدید دستگاه‌های بی‌سیم مخرب، کنترل پورت‌های کابلی است. برای این منظور، پروتکل 802.1x در کنار EAP برای کنترل دسترسی مبتنی بر پورت و احراز هویت در شبکه‌های محلی استفاده می‌شود. همچنین، از 802.1X/EAP برای صدور مجوز دسترسی از طریق پورت‌های کابلی روی یک سوئیچ لایه‌ی دسترسی استفاده می‌شود. روش‌های EAP-MD5 و EAP-TLS می‌توانند برای احراز هویت مبتنی بر 802.1X/EAP و کنترل دسترسی در بخش کابلی شبکه استفاده شوند. همان‌گونه که در شکل (۳) نمایش داده شده است، تا زمانی که داده‌های معتبر برای احراز هویت از سوی متقاضی متصل به پورت لایه‌ی ۲ ارایه نگردد، ارتباطات لایه‌های بالاتر از طریق پورت کابلی مقدور نخواهد بود.

[1] Wireless Intrusion Detection/Prevention System (WIDS/WIPS)



شکل (۳) : پیشگیری از دستگاه‌های بی‌سیم مخرب با به کارگیری 802.1X/EAP در زیرساخت کابلی شبکه

لازم به ذکر است که اغلب سازمان‌ها فاقد راه حل 802.1X/EAP برای کنترل پورت کابلی هستند. از این رو، راه حل دومی که برای مقابله با دستگاه‌های بی‌سیم مخرب به کار می‌رود، استفاده از مکانیزم‌های پایش امنیت مانند سیستم‌های تشخیص/جلوگیری از نفوذ بی‌سیم در شبکه‌ی محلی بی‌سیم است. این سیستم‌ها می‌توانند تهدید بالقوه‌ی ناشی از نقاط دسترسی و ایستگاه‌های بی‌سیم مخرب را شناسایی و خنثی سازند. سیستم‌های جلوگیری از نفوذ از متدهای گوناگونی برای متوقف و قرنطینه نمودن ارتباطات دستگاه‌های مخرب در شبکه‌های محلی بی‌سیم استفاده می‌کنند. در شایع‌ترین روش، مکانیزم جلوگیری از سرویس در لایه‌ی ۲ برای قرنطینه نمودن دستگاه مخرب پس از شناسایی به کار گرفته می‌شود. به این ترتیب، ایستگاه‌ها و نقاط دسترسی غیرمجاز تا زمانی که محل آن‌ها شناسایی شده و از شبکه خارج شوند، به طور مؤثری مهار می‌شوند.

تکنیک دیگری که توسط این سیستم‌ها برای مقابله با تهدید دستگاه‌های غیرمجاز استفاده می‌شود، به‌کارگیری پروتکل SNMP است. به این ترتیب که پس از این که سیستم تشخیص داد نقطه‌ی دسترسی مخربی به زیرساخت

کابلی شبکه متصل گردیده است، با استفاده از پروتکل SNMP پورت متصل به نقطه‌ی دسترسی بی‌سیم مخرب در *سوئیچ مدیریتی*[1] غیرفعال می‌گردد. با غیرفعال شدن این پورت، مهاجم قادر نخواهد بود منابع شبکه‌ی قرار گرفته در پشت نقطه‌ی دسترسی مخرب را مورد حمله قرار دهد. این روش مقابله با دستگاه‌های مخرب به *مهار درگاه*[2] مشهور است.

۳- حمله‌ی مردی در میانه (MitM)

یک نقطه‌ی دسترسی بی‌سیم ممکن است توسط یک مهاجم خارجی و با اهداف بدخواهانه به کار گرفته شود. در این حمله مهاجم با فریب کاربران شبکه‌ی بی‌سیم، اتصال آن‌ها را از نقطه‌ی دسترسی اصلی قطع و سپس، اتصال آن‌ها را با نقطه‌ی دسترسی جعلی مشابه که خود برپا نموده، برقرار می‌کند. حمله‌ی مردی در میانه در شبکه‌های محلی بی‌سیم تهدیدی جدی قلمداد می‌شود که زمینه‌ساز تهدیدها و حملات پیشرفته‌تر است. این حمله به حمله‌ی Evil twin و حمله‌ی Wireless hijacking نیز مشهور است. از نام‌های دیگر این حمله می‌توان به WiFi Phishing، AP Phishing، Honeypot AP و Hotspotter اشاره کرد [2].

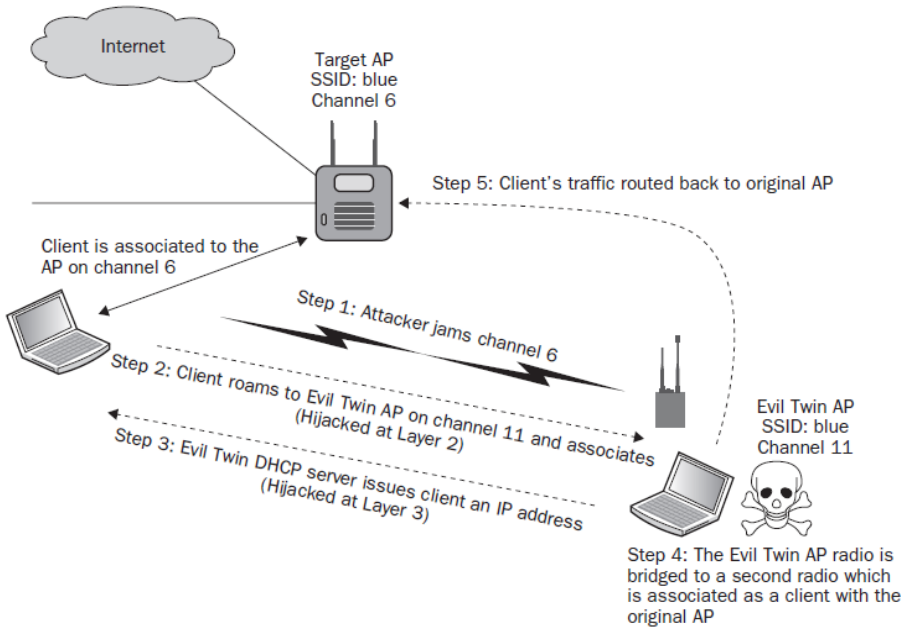
برای انجام این حمله، مهاجم یک نقطه‌ی دسترسی بی‌سیم نرم‌افزاری را با کمک لپ‌تاپ خود پیکربندی و راه‌اندازی می‌کند. در واقع با این کار، مهاجم کارت بی‌سیم لپ‌تاپ خود را به یک نقطه‌ی دسترسی بی‌سیم نرم‌افزاری تبدیل می‌کند. برخی دستگاه‌های بی‌سیم USB نیز قابلیت این را دارند که به عنوان نقطه‌ی دسترسی بی‌سیم عمل کنند. نقطه‌ی دسترسی نرم‌افزاری بر روی لپ‌تاپ مهاجم به گونه‌ای پیکربندی می‌شود که دارای SSID یکسان با نقطه‌ی دسترسی اصلی باشد. نقطه‌ی دسترسی مهاجم اکنون به عنوان یک همزاد بدخواه برای نقطه‌ی دسترسی اصلی عمل می‌کند. نقطه‌ی دسترسی جعلی امواج رادیویی را بر روی کانالی متفاوت با نقطه‌ی دسترسی اصلی ارسال می‌کند. سپس، مهاجم با ارسال فریم‌های *قطع اتصال*[3] برای ایستگاه‌های مشتری باعث قطع اتصال آن‌ها از نقطه‌ی دسترسی مجاز اصلی و اتصال مجددشان به نقطه‌ی دسترسی مخرب خود می‌شود. اکنون مهاجم موفق به ربودن اتصال بی‌سیم

[1] Managed switch
[2] Port suppression
[3] Dis-association

قربانیان از نقطه‌ی دسترسی بی‌سیم مجاز اصلی در لایه‌ی ۲ گردیده است. علاوه بر فریم‌های قطع اتصال، ارسال‌کننده‌های پارازیت رادیویی نیز می‌توانند برای قطع اتصال قربانیان در لایه‌ی ۲ به کار گرفته شوند.

مهاجم پس از دزدیدن اتصال کاربران به منظور تخصیص IP به ایستگاه‌های بی‌سیم متصل شده، معمولا اقدام به نصب و پیکربندی یک سرویس‌دهنده‌ی DHCP بر روی نقطه‌ی دسترسی جعلی خود می‌نماید. در این صورت، مهاجم موفق به دزدیدن اتصال بی‌سیم قربانیان در لایه‌ی ۳ می‌شود. اکنون مهاجم یک شبکه‌ی محلی بی‌سیم اختصاصی در اختیار دارد و قادر خواهد بود حملات بیشتری از نوع نظیر به نظیر بر روی هر یک از ایستگاه‌های قربانی انجام دهد که شرح آن در بخش ۳-۳ خواهد آمد.

یک مهاجم با به کارگیری یک کارت بی‌سیم دیگر روی لپ‌تاپ خود قادر خواهد بود حمله‌ی مردی در میانه را تکمیل کند. شکل (۴) مراحل انجام این حمله را نمایش می‌دهد. همان‌گونه که در این شکل نمایش داده شده است، کارت واسط بی‌سیم دوم به عنوان یک ایستگاه عادی به نقطه‌ی دسترسی اصلی متصل می‌شود. مهاجم می‌تواند کارت‌های بی‌سیم دوم و اولی که به عنوان نقطه‌ی دسترسی مخرب به کار گرفته شده است را پل نماید. به این ترتیب، پس از ربوده شدن اتصال بی‌سیم کاربر از نقطه‌ی دسترسی اصلی، ترافیک قربانی از نقطه‌ی دسترسی مخرب و از آن‌جا از طریق کارت واسط دوم دوباره به نقطه‌ی دسترسی اصلی یعنی نقطه‌ای که اتصال از آن‌جا دزدیده شده بود، باز می‌شود. در نتیجه، کاربران مورد حمله قرار گرفته، همچنان مسیری برای عبور ترافیک خود به شبکه‌ی اصلی اولیه خواهند داشت و این بدان معنی است که قربانیان هرگز متوجه نخواهند شد مورد حمله قرار گرفته‌اند. به عنوان مثال، در حالتی که شبکه‌ی اصلی سرویس اینترنت را برای کاربران فراهم می‌نماید، با وقوع حمله‌ی مردی در میانه بی‌سیم همچنان اتصال اینترنت حفظ خواهد شد. بنابراین، مهاجم می‌تواند بدون این که شناسایی گردد، در بین ارتباط قرار گرفته و بدون محدودیت به انجام حملات نظیر به نظیر بپردازد.



شکل (۴) : حمله‌ی مردی در میانه بی‌سیم

۳-۱- آسیب‌پذیری فریم‌های مدیریتی 802.11

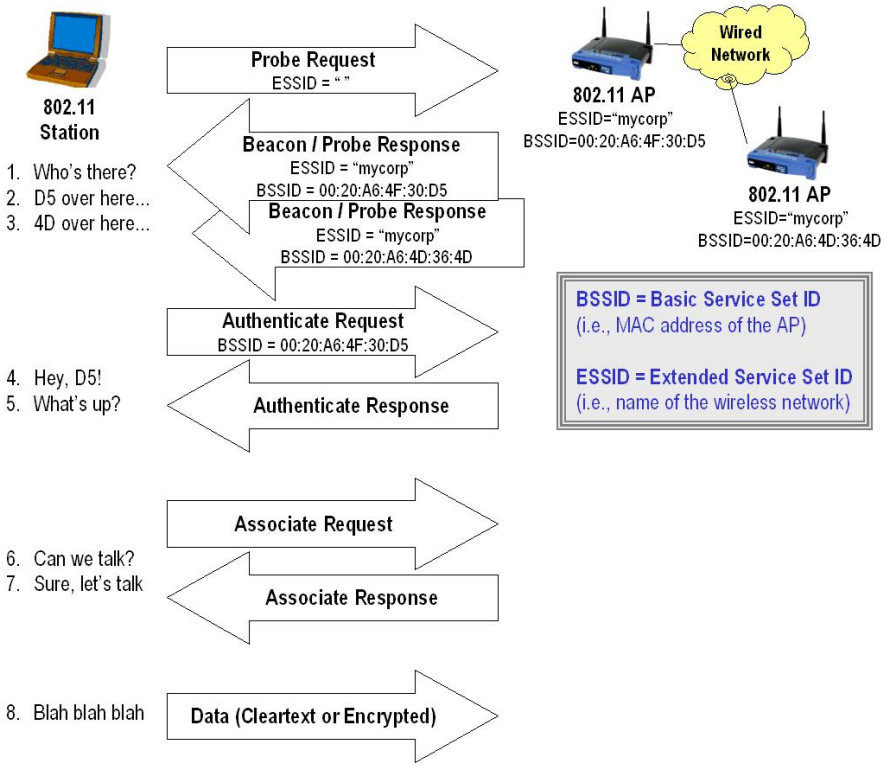
در این بخش به تشریح نقطه‌ی آسیب‌پذیر موجود که سنگ‌بنای شکل‌گیری حمله‌ی مردی در میانه در شبکه‌های محلی بی‌سیم است، پرداخته می‌شود. فریم‌های مدیریتی 802.11 به سادگی قابل جعل بوده و نقاط دسترسی مکانیزمی برای تایید هویت فرستنده‌ی آن‌ها ندارند. همچنین، در داخل یک شبکه‌ی محلی بی‌سیم، ایستگاه‌های بی‌سیم مشتری مانند لپ‌تاپ‌ها، PDAها و تلفن‌های هوشمند به طور خودکار نقطه‌ی دسترسی بی‌سیمی را که توان سیگنال بهتری دارد انتخاب کرده و به آن متصل می‌شوند. این موضوع مشکل را دو چندان کرده و زمینه‌ساز سوءاستفاده‌ی مهاجمین در ربودن اتصال بی‌سیم کاربران مجاز می‌گردد. برای درک بیشتر آسیب‌پذیری منجر به وقوع این حمله، در ادامه مقدمه‌ای بر فریم‌های مدیریتی، نحوه‌ی احراز هویت و مراحل اتصال کاربران بی‌سیم به نقطه‌ی دسترسی آورده شده است.

دو نوع از فریم‌های مدیریتی 802.11 که برای آشنایی اولیه بین ایستگاه‌ها و نقاط دسترسی رد و بدل می‌شوند عبارتند از فریم‌های beacon و probe. فریم‌های beacon به طور مستمر توسط هر نقطه‌ی دسترسی بی‌سیم در محیط فرستاده می‌شوند تا علاوه بر اعلام وجود نقطه‌ی دسترسی، مشخصات شبکه‌ی بی‌سیم مربوطه نیز در اختیار سایر ایستگاه‌های مجاور قرار گیرد. فریم‌های beacon و probe حاوی اطلاعاتی مانند نام شبکه‌ی بی‌سیم (ESSID)، آدرس MAC مربوط به نقطه‌ی دسترسی (BSSID) و نام الگوریتم رمزنگاری استفاده شده هستند. به این ترتیب،

ایستگاه‌ها می‌توانند به طور غیرفعال یعنی بدون فرستادن حتی یک فریم، از مشخصات نقاط دسترسی مجاور آگاه شوند. فریم‌های probe دارای دو نوع probe request و probe response می‌باشند که اولی توسط ایستگاه‌ها برای شناسایی شبکه‌های بی‌سیم مجاور به طور فعال و دومی توسط نقاط دسترسی و در پاسخ به این درخواست‌ها فرستاده می‌شوند. بسته‌های probe می‌توانند به طور خاص برای شناسایی شبکه‌های بی‌سیم ذخیره شده یا به طور عام برای آگاهی از وجود همه‌ی نقاط دسترسی ممکن ارسال شوند. هیچ مکانیزم رمزنگاری برای محافظت از محتویات این فریم‌های مدیریتی وجود ندارد. همچنین، ایستگاه‌ها و نقاط دسترسی قادر به تایید هویت فرستنده‌ی آن‌ها نیستند. این بدان معنی است که مهاجمین به راحتی قادرند محتویات فریم‌های مدیریتی 802.11 را مشاهده، جعل و یا دستکاری نمایند.

پس از این که یک ایستگاه مشتری به کمک فریم‌های beacon و probe از شبکه‌های موجود اطلاع یافت، نوبت به انتخاب یک شبکه‌ی هدف و اقدام برای اتصال به آن است. فرآیند اتصال عموما با ارسال فریم *درخواست احراز هویت*[1] آغاز می‌شود، ولی بسته به مکانیزم احراز هویت استفاده شده توسط نقطه‌ی دسترسی بی‌سیم متفاوت خواهد بود. در ساده‌ترین حالت، یعنی روش *احراز هویت باز*[2] فقط ۲ فریم درخواست احراز هویت و پاسخ درخواست برای احراز هویت رد و بدل می‌شوند. در این روش، هر درخواست اتصالی پذیرفته شده و هر ایستگاه متقاضی می‌تواند به شبکه‌ی بی‌سیم متصل شود. پس از احراز موفقیت‌آمیز هویت مشتری توسط نقطه‌ی دسترسی، عملیات اتصال با رد و بدل فریم‌های *ثبت اتصال*[3] انجام می‌گیرد. شکل (۵) مراحل آشنایی، احراز هویت باز و اتصال یک ایستگاه مشتری به یک نقطه‌ی دسترسی بی‌سیم را نشان می‌دهد. رویه‌ی اتصال در سایر مکانیزم‌های رمزنگاری مانند WEP و WPA که از روش‌های احراز هویت *کلید پیش‌اشتراکی*[4] استفاده می‌کنند، متفاوت خواهد بود.

[1] Authentication request
[2] Open authentication
[3] Association
[4] Pre-Shared Key (PSK)



شکل (۵) : مراحل اتصال یک ایستگاه به نقطه‌ی دسترسی بی‌سیم

اکنون به تشریح آسیب‌پذیری‌های موجود در مراحل فوق که باعث شکل‌گیری حمله‌ی Evil twin می‌گردد، پرداخته می‌شود.

- **انتخاب نقطه‌ی دسترسی جهت اتصال فقط بر اساس نام ESSID:** به این معنی که مهاجم با دانستن ESSID مربوط به یک شبکه‌ی محلی بی‌سیم، موفق خواهد شد یک نقطه‌ی دسترسی جعلی و به ظاهر مجاز راه‌اندازی کند. ESSIDها به طور مرتب در شبکه‌ی بی‌سیم اعلام می‌شوند. حتی اگر نقطه‌ی دسترسی به گونه‌ای پیکربندی شود که ESSID را از فریم‌های beacon ارسالی خود حذف نماید (مانند شبکه‌های بی‌سیم مخفی)، ESSID همچنان در فریم‌های probe، احراز هویت و ثبت اتصال رد و بدل خواهد شد.
- **عدم احراز هویت نقاط دسترسی توسط ایستگاه‌ها:** در شبکه‌های بی‌سیم 802.11 هویت نقاط دسترسی با یک آدرس عمومی (آدرس MAC) برای ایستگاه‌ها محرز می‌گردد. اگر چه آدرس‌های MAC سخت‌افزاری و یکتا هستند، با این حال توسط ابزارهای کارت واسط شبکه قابل تغییر هستند. بنابراین، هر ایستگاه بی‌سیم می‌تواند فریمی ارسال کند که به نظر آید از نقطه‌ی دسترسی قانونی ارسال شده است.

- **عدم وجود هیچ مکانیزم رمزنگاری برای محافظت از محتویات فریم‌های مدیریتی beacon و probe در مقابل شنود، دستکاری، تزریق و بازپخش:** مهاجمین به سادگی توسط ابزارهای موجود می‌توانند فریم‌های مدیریتی را ضبط نموده، محتویات آن‌ها را تغییر داده و در زمان مناسب مجدد ارسال نمایند. برای انجام حمله‌ی Evil twin گاهی لازم است اتصال قربانی از نقطه‌ی دسترسی مجاز قطع و مراحل شکل (۵) مجدد انجام پذیرد. مهاجمین این عمل را با فرستادن فریم‌های قطع اتصال انجام می‌دهند.

۳-۲- ربودن اتصال بی‌سیم

عموما هنگامی که یک دستگاه بی‌سیم مشتری مانند لپ‌تاپ روشن می‌شود، به جستجوی شبکه‌های بی‌سیمی می‌پردازد که قبلا به آن‌ها متصل شده است. این شبکه‌ها در فهرستی با نام *فهرست شبکه‌های مرجع*[1] در سیستم‌های عامل مبتنی بر ویندوز ذخیره می‌گردند. به طور همزمان، فهرست تمامی شبکه‌های بی‌سیم تحت پوشش کارت بی‌سیم توسط سیستم عامل نمایش داده می‌شود. یک مهاجم می‌تواند به دو روش اتصال بی‌سیم کاربران را سرقت کند.

در روش اول، مهاجم به گوش دادن فریم‌های probe پرداخته و سپس، یک نقطه‌ی دسترسی جعلی با ESSID یکسان با آن‌چه کاربر در فریم probe request جستجو می‌کند، راه‌اندازی می‌نماید. این امر سبب متصل شدن خودکار کاربر به نقطه‌ی دسترسی جعلی می‌شود، در حالی که کاربر ممکن است حتی از این اتصال بی‌خبر بماند. ابزار Karma از این تکنیک استفاده می‌کند.

ایجاد یک نقطه‌ی دسترسی جعلی با ESSID یکسان با نقاط دسترسی مجاز مجاور، روش دیگری است که یک مهاجم برای گمراه کردن کاربران به منظور متصل شدن آن‌ها به نقطه‌ی دسترسی جعلی، ممکن است به کار گیرد. این‌گونه حملات در مکان‌های عمومی مانند رستوران، کافی‌شاپ و فرودگاه که اشخاص در جستجوی اتصال اینترنت بی‌سیم هستند، شایع‌تر است.

با توجه با این که این حملات در نتیجه‌ی اتصال اشتباهی کاربران به نقطه‌ی دسترسی متعلق به مهاجم روی می‌دهند، حملات Honeypot یا *اتصال اشتباهی*[2] نیز نامیده می‌شوند.

[1] Preferred Network List (PNL)
[2] Mis-association

۳-۳- تهدیدها و آثار مخرب بیشتر

در ادامه، برخی حملات و تهدیدهایی که در پی انجام حمله‌ی مردی در میانه یا همزمان با آن روی می‌دهند، به طور مختصر بررسی خواهند شد.

- **آسیب‌پذیری DHCP:** رایانه‌ی کاربری که در حین اتصال به یک نقطه‌ی دسترسی جعلی است، ممکن است قربانی نوعی از حمله‌ی DHCP نیز گردد. این حمله پس از ربوده شدن اتصال بی‌سیم قربانی و در حین تخصیص IP با به کارگیری آسیب‌پذیری در فرآیند DHCP، قادر خواهد بود کدهای مخرب مانند روت‌کیت را به رایانه‌ی قربانی منتقل نماید.
- **حمله‌ی WiFi Phishing:** دسته‌ی دیگری از حملات که در پی حمله‌ی مردی در میانه رخ می‌دهند، معروف به حملات WiFi Phishing هستند. مهاجم پس از دزدیدن اتصال بی‌سیم، با برپایی یک سرویس‌دهنده‌ی وب مانند IIS یا Apache بر روی سیستم خود، قربانیان را به صفحه‌ی وبی هدایت می‌کند که دقیقا مانند صفحه‌ی ورود شبکه‌های WiFi عمومی به نظر می‌رسد. این صفحه‌ی ورود تقلبی ممکن است برای دزدین نام کاربری، کلمه‌ی عبور و یا حتی شماره‌ی کارت اعتباری به کار گرفته شود.
- **استراق سمع با حمله‌ی مردی در میانه:** با اجرای موفقیت‌آمیز حمله‌ی مردی در میانه، مهاجم که در میان ارتباط قربانیان با نقطه‌ی دسترسی اصلی قرار گرفته است، قادر خواهد بود تمام ترافیک بی‌سیم رمزنگاری نشده را بدون این که کاربران اطلاع یابند، شنود نماید.
- ***ربودن نشست***[1]**:** از حملات جالب دیگری که در پی حمله‌ی مردی در میانه شکل می‌گیرد، ربودن نشست در لایه‌ی کاربرد است. مهاجم با اجرای حمله‌ی مردی در میانه، به تمام ترافیک قربانی در لایه‌ی ۲ دسترسی دارد. این بدان معنی است که ارتباط پروتکل‌ها و برنامه‌های کاربردی قرار گرفته در لایه‌های بالاتر نیز می‌تواند توسط مهاجم متوقف و مورد دستکاری قرار گیرد. برای مثالی از این حمله، سناریویی را در نظر بگیرید که یک بسته حاوی درخواست DNS از ماشین قربانی به مهاجم ارسال می‌گردد. مهاجم با استفاده از برنامه‌ی DNSSpoof یک بسته‌ی حاوی پاسخ DNS ساختگی به ایستگاه قربانی می‌فرستد که در آن آدرس IP ماشین مهاجم متناظر با www.google.com (دامنه‌ی موجود در درخواست DNS فرستاده شده توسط

[1] Session hijacking

کاربر) قرار داده شده است. در واقع، مهاجم این بسته را در بین راهش به سوی سرویس‌دهنده‌ی اصلی DNS متوقف نموده و پاسخ دلخواه خود را به قربانی می‌فرستد. قربانی نیز این پاسخ را پذیرفته و به صفحه‌ی وب مورد نظر مهاجم هدایت می‌شود.

۳-۴- شناسایی و مقابله

تنها راه حل قطعی برای جلوگیری از حملات مردی در میانه بی‌سیم و سایر حملات نشأت گرفته از آن، استفاده از رویکرد *احراز هویت دوطرفه*[1] است. در این راه‌کار نه تنها نقاط دسترسی بی‌سیم هویت ایستگاه‌های مشتری را تصدیق می‌نمایند، بلکه ایستگاه‌های متقاضی نیز پیش از اتصال به شبکه، هویت نقطه‌ی دسترسی را بررسی و تصدیق می‌نمایند. به‌کارگیری راهکار احراز هویت 802.1X/EAP در شبکه‌ی محلی بی‌سیم (استاندارد 802.11i مد سازمانی) الزام می‌دارد که احراز هویت دوطرفه پیش از دسترسی کاربر به شبکه انجام پذیرد. با این روش، کاربر قبل از آن که مجاز شناخته شود، قادر نخواهد بود آدرس IP بگیرد؛ در نتیجه، امکان دزدیده شدن اتصال بی‌سیم و تخصیص IP توسط مهاجم وجود نخواهد داشت.

علاوه بر به‌کارگیری فن‌آوری 802.1X/EAP در بخش بی‌سیم شبکه، همانند آن‌چه در بخش ۲-۴ گفته شد، به‌کارگیری سیستم‌های تشخیص/جلوگیری از نفوذ بی‌سیم نیز در شناسایی و مقابله با تهدید حمله‌ی مردی در میانه مؤثر هستند.

علاوه بر دو مورد پیشگیری قطعی که در بالا آمد، توصیه‌های امنیتی زیر نیز در کاهش احتمال وقوع این حمله مؤثر خواهند بود:

- در مکان‌های عمومی که اینترنت بی‌سیم رایگان ارایه می‌شود، حتی‌الامکان از اتصال به شبکه‌های بی‌سیم خودداری نمایید. از آن‌جا که ریسک اتصال به یک نقطه‌ی دسترسی مخرب در این موارد همواره وجود دارد، استفاده از اینترنت شخصی که ممکن است برای کاربران هزینه داشته باشد، ایمن‌تر خواهد بود.
- در مواقعی که به اینترنت بی‌سیم نیاز ندارید، واسط شبکه‌ی بی‌سیم را غیرفعال نمایید. مادامی که واسط بی‌سیم دستگاه‌هایی مانند تلفن‌های همراه هوشمند و تبلت‌ها که قابل حمل هستند فعال باشد، این دستگاه‌ها

[1] Mutual authentication

در جستجوی شبکه‌های بی‌سیم ذخیره شده‌ی قبل، به طور مرتب فریم‌های probe را در محیط اطراف ارسال می‌کنند. این امر دستگاه بی‌سیم را در معرض اتصال خودکار به نقطه‌ی دسترسی مخرب با نام جستجو شده‌ی مشابه قرار می‌دهد.

- از ابزارهای اتصال امن جهت اتصال به نقاط دسترسی عمومی استفاده نمایید. به عنوان مثال، برنامه‌ای مانند IPASS مشتریان را از طریق یک صفحه‌ی ورود رمزنگاری شده به شبکه متصل می‌نماید که به این ترتیب، تهدید حملات Phishing وب در بستر بی‌سیم را از بین خواهد برد.

۴- نتیجه‌گیری

دستگاه‌های بی‌سیم مخرب و در رأس آن‌ها نقاط دسترسی ممکن است توسط عاملی داخلی (کارمندان سازمان) و یا خارجی (مهاجم) به طور غیرمجاز به کار گرفته شوند. در مورد اول، تهدیدی شکل می‌گیرد که خود شبکه‌ی سازمان را هدف قرار می‌دهد. به‌کارگیری نقطه‌ی دسترسی غیرمجاز توسط یک مهاجم با اهداف بدخواهانه، حمله‌ی مردی در میانه بی‌سیم را شکل می‌دهد که دستگاه‌های مشتریان را مورد هدف قرار می‌دهد. هر دو مورد از تهدیدات جدی و فعال در حوزه‌ی شبکه‌های محلی بی‌سیم تلقی می‌گردند.

مؤثرترین روش برای مقابله با تهدید نقاط دسترسی داخلی مخرب، استفاده از مکانیزم احراز هویت و کنترل دسترسی 802.1x/EAP در سمت کابلی شبکه است. همچنین، اگر 802.1x/EAP در سمت بی‌سیم شبکه به کار گرفته شود، حملات مردی در میانه و دزدیدن اتصال بی‌سیم را متوقف خواهد نمود. روش دیگر برای مقابله با این تهدیدات به‌کارگیری سیستم‌های تشخیص و جلوگیری از نفوذ بی‌سیم است. شناسایی نقاط دسترسی مخرب در حال حاضر از زمینه‌های پژوهشی فعال در حوزه‌ی شبکه‌های بی‌سیم 802.11 است.

مراجع

[1] David Coleman, *CWSP (Certified Wireless Security Professional) Official Guide*, Sybex Publishing , 2010.

[2] http://www.watchguard.com/infocenter/editorial/27061.asp

[3] Vivek Ramachandran, "BackTrack 5 Wireless Penetration Testing Beginner's Guide: Chatper 6 Attacking the Client", 2011

[4] Vivek Ramachandran, Advanced WLAN attacks , 2011.