بسمه تعالی

چالش های امنیتی در شبکه های بیسیم وارائه راه حل پیشنهادی (اثر همسایگی)

حمید رضا هاشمی نژاد ha.hasheminejad@gmail.com

جلال رجائی زاده عضو هیات علمی پیام نور j_rajaeizadeh@pnu.ac.ir

چکیده: پیشرفت شگفت انگیز امکانات مخابراتی ازیک سو باعث گسترش روشهای ارسال ودریافت اطلاعات گردیده واز سوی دیگر پیشگیری از سوء استفاده افراد فرصت طلب را اجتناب ناپذیر نموده است .در این مقاله ابتدا راجع به شبکه های بیسیم و سطوح مختلف امنیتی توضیحات لازم ارائه می گردد ، سپس مشکلی که حتی وجود آن از دید اکثر متخصصان شبکه هم پنهان مانده ، مطرح می شود و راه حل آن هم در ادامه پیشنهاد می گردد.

مقدمه: شبکه ها از نظر بستر و سیستم انتقال به دو دسته با سیم و بیسیم تقسیم می شوند .با توجه به شرایط و ویژگیها ی خاص هر محیطی ،یکی از این دو روش استفاده می شودکه هریک مزایا و معایب مربوط به خود را دارد .شبکه های سیمی باعث ایجاد شبکه های امن تر ، پرسرعت تر و پایدار تری نسبت به شبکه های بیسیم می باشند. از لحاظ دیگر شبکه های بیسیم به علت راحتی در نصب و اجرا در شرایط محیطی خاص که کابل کشی به سهولت انجام نمی شود بهترین گزینه می باشد .همچنین نمی توان قابلیت Mobility آن را به علت پایین بودن امنیت نادیده گرفت .پس بهتر است با دانستن شرایط و موقعیت و اطلاع از موارد امنیتی آن که از مهمترین موضوعات قابل بحث در شبکه های بیسیم می باشد ،بهترین گزینه را برای بستر انتقالی انتخاب نماییم.

سطوح امنیتی در شبکه های بیسیم :

۱) سطح اول: جلوگیری از ورود غیر مجاز به شبکه

۱ ۱) کنترل محدوده پوشش و برد آنتن (Output Power): پیشگیری از دسترسی افراد غیر مجاز مستقر در خارج از محدوده فیزیکی مورد نظر به شبکه.

۱ ۲) ایجاد سطح امنیتی بر روی آدرس یکتای آنتن (Mac ID Filtering): این آدرس برای هرآنتن یکتا است پس می توانیم در آنتن مرکزی تعیین کنیم که چه کاربرانی میتوانند به آن متصل شوند بدین وسیله می توانیم از ورود افراد ناخواسته جلوگیری کنیم.

۱ ۳) تنظیم آنتن فرستنده (Access Point) :استفاده از الگوریتم های رمز نگاری و کلید ها بین گیرنده و فرستنده جهت ارسال و دریافت کلیه پکت های اطلاعات (Data Encryption WEP,WPAv2,…)

۱ ۴) عدم تنظیم آدرس دهی اتوماتیک (DHCP) در شبکه : با این کار شناسائی رنج IP های شبکه از طریق آدرس دهی اتوماتیک (DHCP) مشکل می گردد.

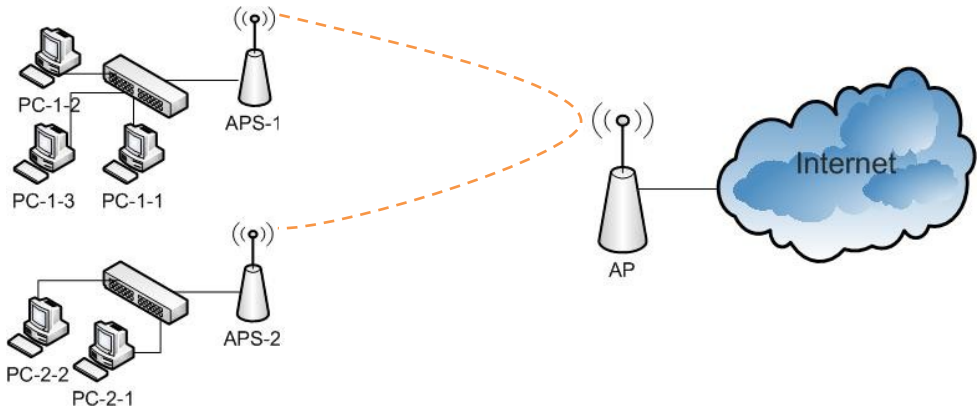
۱ ۵) غیر فعال کردن انتشار نام آنتن فرستنده در محیط (Disable SSID Broadcast)

۲) سطح دوم : پس از ورود به شبکه

گام بعدی در سطوح امنیتی یک شبکه ،امنیت پس از ورود است .اینکه کاربر پس از اتصال به شبکه فقط بتواند به اطلاعات مورد نیاز خود دسترسی داشته باشد نه به اطلاعات کاربران دیگردر همان شبکه . جالب اینجاست که بسیاری تصور می کنند که امنیت فقط به معنای جلوگیری از ورود به شبکه می باشد ولی موضوع اصلی و مشکل اصلی قابل بحث در امنیت پس از ورود به شبکه هم می باشد.

موضوع اصلی این مقاله طرح و بررسی این مهم است و سپس پیشنهاد راهکار مناسب برای رفع این مشکل می باشد.

فرض کنید دو ایستگاه گیرنده (Access Point Station) قصد دارند جهت اتصال به اینترنت (یا هر منبع دیگری) به شبکه متصل گردند.



تصویر شماره ۱ (توپولوژی شبکه بیسیم)

این دو کاربر از لحاظ سطح امنیتی ۱ (سطوح توضیح داده شده) با اجازه کامل مدیر شبکه وارد شبکه می شوند و هر دو می بایست در آنتن فرستنده تعریف شوند تا بتوانند از منابعی که فرستنده در اختیار دارد استفاده نمایند (مثل اینترنت).

اولین مرحله امنیتی (از نظر این مقاله) به خوبی پیاده سازی شده است و از ورود افراد متفرقه به شبکه جلوگیری می کند.

مرحله بعدی و موضوع جالب این است که پس از اتصال این دو کاربر به شبکه برروی یک آنتن فرستنده ،هر دو به راحتی و بدون اجازه مدیر شبکه میتوانند با استفاده از بستر ارتباطی فعلی به منابع همدیگر دسترسی داشته باشند !!!

موضوع با یک مثال واضح تر بررسی می شود:

در همان شبکه بالا تصور کنید مدیر شبکه بخواهد این دو کاربر پس از اتصال به آنتن اصلی هر کدام به اندازه ۵۱۲ کیلو بیت از اینترنت استفاده نمایند یعنی هر کدام در بهترین حالت میتوانند از ۵۱۲ کیلو بیت از این بستر ارتباطی بیسیم استفاده نمایند .مدیرشبکه میتواند بااستفاده از ابزار های کنترلی و برنامه

های کنترل پهنای باند روی روتر ،میزان دسترسی به اینترنت را محدود سازد .ولی جالب اینکه اگر PC-1-1 بخواهد از طریق آنتن خود (APS-1) با PC-2-1 با آنتن (APS-2) جهت استفاده از منابع یکدیگر ارتباط برقرار کند با سرعت بیش از ۵۱۲ کیلو بیت و حتی بیشتر از آن می توانند در این شبکه فعالیت کنند .جالب اینجاست که نه باسرعت ۵۱۲ کیلو بیت بلکه با نهایت سرعت آنتن فرستنده (Capacity) شروع به ارسال و دریافت و استفاده از منابع یکدیگر به دور از چشم مدیر شبکه و برنامه های کنترل شبکه (Network Monitoring) می کنند و دیگر پهنای باند در نظر گرفته شده در شبکه به دلیل داخلی بودن (عدم عبور پکت در داخل روتر) نادیده گرفته می شود و این یکی از بزرگترین معزل هایی می باشد که می تواند در شبکه اختلال ایجاد کند .

دو کاربر می توانند با استفاده از نهایت پهنای باند این بستر ارتباطی ، فعالیت نمایند و حتی میتوانند بستر بوجود آمده از آنتن فرستنده را با استفاده از برنامه های مخرب همانند WAN Killer ها به راحتی مورد هجوم قرار دهند و بدیهی است که اینگونه برنامه های مخرب بر روی دیگر کاربران که از آن آنتن فرستنده سرویس می گیرند اثر منفی می گذارد .مثلا احتمال به تعلیق در آمدن و از کار افتادن آنتن اصلی می باشد که فعالیت دیگرکاربران راهم تا زمان Reset نشدن آنتن مختل می کند .

این مشکل زمانی حساس تر می شود که برای مثال یک سیستم حاوی اطلاعات بسیار مهم و محرمانه یک سازمان روی آنتن گیرنده APS-1 قرار داشته باشد و برروی آنتن گیرنده APS-2 کاربران عادی که هرگز نباید به آن اطلاعات مهم دسترسی داشته باشند جهت برقراری ارتباط با اینترنت متصل شده اند. موضوع به این صورت است که قرار است هر دو کاربر به شبکه اینترنت متصل گردند ولی آنها به منابع یکدیگر و سیستم های یکدیگر دسترسی نداشته باشند .مثلا در این سناریو کاربر عادی نباید در سطح امنیتی (داخل یک LAN) کامپیوتر حاوی اطلاعات بسیار مهم و محرمانه باشد در حالیکه این کاربر در زمان وارد نمودن اطلاعات مهم باشد .

به بیان دیگر این موضوع دقیقا همانند زمانی است که شما و شخص دیگری در پوشش یک محدوده آنتن مخابراتی ارتباط سیار (BTS) قرار گرفته اید این مشکل زمانی به یک معزل تبدیل می شود که شما بتوانید بدون پرداخت هزینه (Billing) با هم ارتباط برقرار کنید .

پیشنهاد راه حل های این مشکل بزرگ

خوشبختانه طبق تحقیقات به عمل آمده از مدیران شبکه و تعداری از کاربران ،افراد کمی از چنین مشکلی در شبکه های بیسیم مطلع هستند .

لازم است این بستر ارتباطی را با بستر ها و تکنولوژی های ارتباطی مورد ارزیابی قرار داده سپس راه حل مناسب ارائه شود.

شبکه های کابلی با سوئیچ لایه ۲ (Manageable Switch)

شبکه هایی که در انتهای اتصال به یک سوئیچ قابل برنامه ریزی منتهی می گردد(نه به هاب سوئیچ های لایه ۱ و غیر قابل برنامه ریزی)

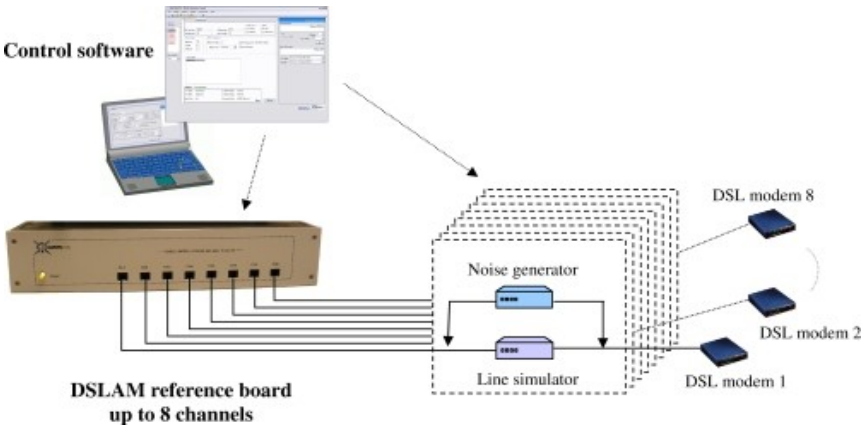
اگر در یک شبکه از یک Switch قابل برنامه ریزی (Manageable) استفاده نماییم به راحتی میتوانیم اول با استفاده از MAC Table برای هر سیستم فقط یک پورت خاص اختصاص دهیم و سپس با استفاده از Bandwidth پهنای آن پورت را به راحتی کنترل کنیم که حتی باپورت های همسایه هم با بیش از این سرعت نتوانند ارتباط برقرار کنند .

همچنین می توانیم در Switch با استفاده از تعریف (VLAN (Virtual LAN دسترسی پورت ها به همدیگر را هم کنترل و محدود نماییم .

تکنولوژی DSL مثلا شبکه ADSL شهری و دستگاه DSLAM

ابتدا در مورد ساختار ارتباطی شبکه ADSL را بررسی می کنیم و سپس این مشکل همسایگی را در آن بررسی می کنیم .

شبکه ADSL برروی دستگاهی بنا شده است که DSLAM (Digital subscriber line access multiplexer) نامیده می شود . این دستگاه در انواع مختلفی تولید می شود و دارای قابلیت های گوناگونی می باشند ولی جهت درک بهتر برروی انواع ساده مشکل را بررسی می کنیم .



تصویر شماره ۲ (دستگاه DSLAM با پورت های RJ11)

دستگاه DSLAM پس از قرار گیری در محل تجمع کابل های تلفن متقاضیان (مثلا مرکز مخابراتی) هر کابل تلفن به یک پورت این دستگاه متصل یا اصطلاحا رانژه می شود .

حال فرض کنید خط تلفن شما روی پورت ۱ و خط مشترک بعدی روی پورت ۲ باشد . تصور کنید پس از برقراری اتصال مشترک پورت ۲ به راحتی میتواند به اطلاعات Share

شده و منابع روی سیستم پورت ۱ دسترسی داشته باشد .از این رو این دستگاه ها در دو مد اصلی طراحی و ساخته می شوند .

۱) مد محدود (Restricted)

۲) مد نا محدود (Unrestricted)

تفاوت این دو در این است که در حالت اول تمامی پورت ها فقط و فقط می توانند با پورت اصلی Ethernet دستگاه DSLAM کار کنند و اینترنت بگیرد ولی در مد دوم تمامی پورت ها هم میتوانند به راحتی با یکدیگر تبادل اطلاعات نمایند و هم از پورت اصلی Ethernet دستگاه سرویس بگیرند.

راه حل های پیشنهادی جهت جلوگیری اثر همسایگی در شبکه های بی سیم

طبق مقایسه های انجام شده به علت عدم وجود پورت خاص یا رابط مجزا (Interface) برای هر مشترک قادر به تصمیم گیری روی هر مشترک و کاربر نیستیم ولی می توانیم به راحتی از مشخصه های دیگر یک ارتباط بیسیم استفاده نماییم . (MAC Spoofing)

از مشخصه های یکتای یک ارتباط بیسیم که اساس و پایه ارتباط هم می باشد MAC Address آنتن گیرنده می باشد . بدین صورت می توانیم به راحتی با استفاده از این مشخصه که در کل دنیا برروی هر آنتن یکتا می باشد وهمچنین جلسه (Session) ایجاد شده برروی آنتن فرستنده تصمیماتی اتخاذ نماییم .بدین صورت که می توانیم برای هر کاربر با استفاده از شناسه های نام برده یک عدد رابط مجازی (Virtual Interface) ایجاد نماییم .در این صورت می توانیم کلیه محدودیت ها (Restricted) و مدیریت ها را برروی این اینترفیس اعم از پهنای باند و غیره اعمال نماییم.

منابع:

1- Institute of Electrical and Electronics Engineers (www.IEEE.org) -Digital Object Identifier 10.1109/IAW.2005.1495946

2- Internet Engineering Task Force (www.ietf.org) -Mobile and Wireless Networks Security 2009