نقش سرور ریدیوس در شبکه‌های بی‌سیم محلی

پوهنیار سیدعابد سادات و پوهندوی امیرکرور شهیدزی[٦]
تقریظ دهنده: پوهندوی عبدالرحمن مجددی

مجله‌ی علمی-تحقیقی حوزه‌ی علوم طبیعی پوهنتون کابل، ۳ (٤) ۱٤۰۰

چکیده

این تحقیق نقش اساسی سرور امنیتی RADIUS را بالای تکنالوژی‌های شبکه‌های بی‌سیم محلی با استفاده از تخنیک‌های امنیتی مدل AAA بررسی می‌کند. از روش تحقیق آزمایشی و پیشینه‌ی تحقیق برای جمع‌آوری اطلاعات درین مورد استفاده شده است. با استفاده از سرور RADIUS، هر کاربری که بخواهد، به سیستم شبکه‌های بی‌سیم محلی وصل گردد نیاز است تا سرتفیکیت مخصوص را در وسیله‌ی خود نصب کرده و از اسم و رمز عبور که در دومین این سرور است، به آن معرفی کرده و به شبکه بی‌سیم وصل گردد. و هر کاربر اسم و رمز عبور جداگانه و مشخص نیاز دارد که اشخاص غیرمجاز نتوانند وارد شبکه‌ی بی‌سیم گردند؛ چون احراز هویت و تعیین حدود صلاحیت توسط Access Point صورت نمی‌گیرد بل‌که از سرور RADIUS عملیات احراز هویت و تعیین حدود صلاحیت از یک نقطه‌ی مرکزی با امنیت بالا صورت می‌گیرد.

اصطلاحات کلیدی: امنیت شبکه؛ Access Point؛ دومین امنیتی؛ AAA؛ Active Directory

Role of RADIUS Server in Wireless LAN Networks

Jr. Teaching Asstt. Said Abid Sadat and Asstt. Prof. Amir Kror Shahidzay

Abstract

This research explains the main role of the RADIUS security server on Wireless LAN networks using AAA security techniques which controls access of users. In this research experimental research method and literature review have been used to collect information. By using the RADIUS server, any user who wants to connect to the local wireless network systems needs to install a private certificate on device and provide the username and password which are in the domain of the server and connect them to the Wireless networks. And each user needs a separate username and password which unauthorized users cannot access to the wireless LAN devices, whereas, the authentication and authorization processes are not done by the Access Point, but the authentication and authorization is done by the RADIUS server from a central point of access with a high level of security.

Keywords: Network Security; Access Point; Security Domain; AAA; Active Directory

ارجاع

سادات، سیدعابد و شهیدزی، امیرکرور. (۱٤۰۰). نقش سرور ریدیوس در شبکه‌های بی‌سیم محلی. مجله‌ی علمی- تحقیقی حوزه‌ی علوم طبیعی پوهنتون کابل، شماره ۳ (٤)، صص ۷۹-۸۸.

---

[٦] استادان پوهنځی کمپیوترساینس، پوهنتون کابل

مقدمه

افزایش استفاده از شبکه‌های بی‌سیم در شهرها و به‌خصوص نقاط مزدحم تجارتی، در برخی اوقات باعث به وجود آمدن مشکلات بسیاری برای صاحبان شبکه‌های بی‌سیم شده است (۱). در اغلب موارد که این شبکه‌ها مربوط به دفاتر کوچک و یا شرکت‌ها هستند، طراحی نادرست و عدم رعایت موارد امنیتی باعث امکان نفوذ می‌شود. نفوذ در این موارد، علاوه برامکانِ به خطرافتادن اطلاعات داخل سازمان، می‌تواند باعث سوءاستفاده از امکانات شبکه، مانند استفاده از انترنت رایگان بی‌سیم شود. در سال‌های اخیر تکنالوژی بی‌سیم سهولت‌های بیشتر را نسبت به تکنالوژی کیبلی فراهم نموده است و در عموم بسیاری از دفاتر، پوهنتون‌ها، شرکت‌ها و غیره از شبکه‌های بی‌سیم استفاده می‌نمایند و هم‌چنان افراد مغرض مثل حمله‌کننده‌ها (Attackers) در صدد این هستند تا با حمله به سیستم‌ها اطلاعات آن‌ها را بنابر دلایل مختلف تغییر بدهند، کاپی نمایند و یا پاک نمایند (۲).

در شبکه‌های کیبلی می‌توان با قراردادن وسایل فزیکی مثل سویچ، روتر وهاب در نقاط امن و در نظر گرفتن مسیر درست کیبل‌ها از دست‌رسی اشخاص غیرمجاز، بخشی از امنیت آن‌را تأمین کرد، اما در شبکه‌های بی‌سیم محلی زمانی‌که یک Access Point شروع به سرویس‌دهی می‌کند هر کسی که در ساحه‌ی تحت پوشش آن قرار داشته باشد برای آن قابل رویت می‌باشد و خطر ورود غیرمجاز اشخاص درآن امکان‌پذیراست. بناءً، نیاز است که در عرصه‌ی امنیت شبکه‌های بی‌سیم کار صورت بگیرد و موقع اتصال به یک شبکه‌ی بی‌سیم از شما رمز عبور شبکه پرسیده می‌شود تا اجازه‌ی اتصال به شبکه‌ی بی‌سیم میسر شود این رمز به صورت مستقیم از روی Access Point شبکه‌ی بی‌سیم شما قابل تنظیم است اما این رمز عبور بسیار آسیب‌پذیر می‌باشد و یک نفوذکننده‌ی حرفه‌یی خیلی راحت می‌تواند امنیت شبکه‌ی بی‌سیم شما را بشکند و وارد شبکه‌ی بی‌سیم شود (۳). پروتکل RADIUS برگرفته شده از (Remote Authentication Dial-In User Service)، استندردی برای طراحی و پیاده‌سازی سرویس‌دهی است که مسوولیت تأیید و مدیریت کاربران را برعهده دارد (۴). از آن‌جا که شبکه‌های بی‌سیم، دردنیای کنونی بسیار سریع در حال گسترش هستند، مهم‌ترین نکته در راه استفاده از این تکنالوژی، آگاهی از نقاط قوت و ضعف آن است. در مجموع در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی نقاط مشترک موجود است و مشکل عمده شبکه‌های بی‌سیم ورود اشخاص غیر مجاز به شبکه‌ی بی‌سیم می‌باشد. زمانی‌که یک Access Point در یک ارگان یا دفتر شروع به سرویس‌دهی می‌نماید، تمام افراد که در ساحه‌ی تحت پوشش آن قرار دارند در صورتی‌که اطلاعات امنیتی برای ورود به شبکه را داشته باشند، می‌توانند به شبکه وصل گردند (۵).

بناءً، کاربران از یک رمز استفاده می‌کنند که این خود کار نفوذکنندگان را سهل می‌نماید و به آسانی می‌توانند به شبکه نفوذ کنند و مشکل دیگر در شبکه‌های بی‌سیم این‌ست که هرگاه در شبکه چندین Access Point داشته باشیم هر یک از آن‌ها اطلاعات امنیتی به‌خصوص خود را دارند و کار احراز هویت در آن‌ها بخ‌شکل پراکنده و جدا می‌باشد و یک نقطه‌ی مرکزی برای احراز هویت نداریم، بناءً، کاربران را با مشکل مواجه می‌سازد (٦).

پیشینه‌ی تحقیق

شبکه‌های بی‌سیم در کشورهای جهان پیشرفته اکثراً جاگزین شبکه‌های کیبلی گردیده است، و به سرعت در کشورهای‌های جهان سوم در حال گسترش می‌باشد، در کشورهای پیشرفته عموماً تمام امورزندگی خود را با تکنالوژی وفق داده اند (۷).

مردم در کشورهای پیشرفته تمام خرید و فروش اجناس مورد ضرورت در زندگی خود را به‌طور آنلاین انجام می‌دهند و با استفاده از کارت‌های هوشمند داد و ستد می‌نمایند و برای درتماس بودن با یک‌دیگر شان معلوم داراست که از یک شبکه استفاده می‌کنند؛ مثل شبکه‌ی بزرگ انترنت و برای وصل شدن به انترنت از موبایل‌های هوشمند و کمپیوتر استفاده می‌نمایند و برای این‌که همیشه با انترنت وصل باشند نسبت به شبکه‌ی کیبلی، شبکه‌ی بی‌سیم سهولت بیشتر دارد مثل Mobility که در ساحه‌ی پوشش یک شبکه‌ی بی‌سیم می‌توان حرکت داشت و به شبکه وصل باشید و خدمات را در هرمکان تحت پوشش شبکه‌ی بی‌سیم دریافت کرد و بنابرهمین نوع سهولت‌های شبکه‌ی بی‌سیم نسبت به شبکه‌ی کیبلی است که از آن بیشتراستفاده می‌گردد و نفوذکنندگان همیشه در صدد این هستند که تا اطلاعات ضروری و مهم کاربران را از شبکه سرقت نمایند، به این دلیل کارهای زیاد در عرصه‌ی امنیت شبکه‌های بی‌سیم صورت گرفته تا کاربران با اطمینان کامل از شبکه‌های بی‌سیم استفاده نموده و از آن در پیشبرد امور زندگی و کاری خود بکار گیرند (۸). چون سرور RADIUS برای بالا بردن سطح امنیتی استفاده از شبکه‌های بی‌سیم استفاده می‌گردد. سرور RADIUS شناسایی کاربرها هم در شبکه‌های کیبلی و هم در شبکه‌های بی‌سیم ضرور می‌باشد، چون در شبکه‌های بی‌سیم شناسایی کاربرها بیشتر مهم است، به‌خاطر که در شبکه‌های کیبلی دست‌رسی محدودتر می‌باشد و زمانی‌که وسیله‌یی به سرور به‌شکل بی‌سیم وصل گردد، بدون کدام روش خاص برای شناسایی احتمال این‌که نفوذکننده وارد شبکه شده و آسیب‌های جدی را با نفوذ کردن در سیستم برساند است (۹). RADIUS یک پروتکل Authentication, Authorization, Accounting (AAA) است و جای‌گزین اصلی +TACACS برای ارائه‌ی یک نقطه‌ی دست‌رسی متمرکز می‌باشد و تفاوت

اصلی میان این دوتا این است که RADIUS از پروتکل UDP برای برقراری ارتباط بین RADIUS client و RADIUS server استفاده می‌کند(۸).

کاسیولیانس(۲۰۱٦) مفهوم سرور RADIUS را چنین ارائه کرده است؛ شبکه‌ی محلی شامل وسایل فیزیکی و کیبل‌ها می‌باشد که کاربران را با هم دیگر نزدیک ساخته و یک محیط مصوون برای‌شان فراهم می‌نماید. درحالی‌که شبکه‌ی محلی بی‌سیم (WLAN) بر اساس همان اصل کار می‌کند، ولی تا هنوز در معرض دید و دست‌رسی افراد غیر مجاز قرار دارد (۱۰). Access Points به عنوان فرستنده‌ها و گیرنده‌های رادیویی کوچک با فرکانس و محدوده‌ی خاصی کار می‌کنند و این اجازه را می‌دهند تا وسایل که در ساحه‌ی تحت پوشش Access Points است به آن‌ها وصل گردند و هدف عملی این تحقیق عبارت از تطبیق network access control همراه با یک RADIUS Server بیرونی است و مزایای این میتود استفاده از یک سرور بیرونی RADIUS Server است که با استفاده از آن دست‌رسی کاربرها را می‌توان کنترل نموده و از معرض دید افراد غیر مجاز شبکه‌ی بی‌سیم خود را پنهان کرد (۱۱).

تحقیقات نشان داده است که سرور RADIUS پیام‌های Extensible Authentication Protocol (EAP) تماماً توسط یک کارت هوشمند که به‌نام EAP-Servers یاد می‌کنند، پروسس می‌گردد و با استفاده از کارت هوشمند تماماً احراز هویت کاربران توسط RADIUS Server اداره می‌گردد (۱۲).

دیشموخ (۲۰۱۲) در بخش سرور حساب RADIU تحقیق نموده و چنین نوشته است RADIUS Accounting Server برای دریافت یک Accounting Request و دوباره جواب دادن آن به کاربر استفاده می‌شود و زمانی‌که یک کاربر بخواهد از RADIUS Accounting استفاده نماید نخست این کاربر Accounting Requests را به سمت Accounting Server ارسال می‌کند (۱۳). و در صورتی‌که Accounting Server جواب ندهد و یا خاموش شده باشد، کاربر تا یک زمانی معین Requestها را نگه‌داری می‌کند و زمانی‌که سرور فعال گردید، کاربر تمام تقاضاها را فشرده کرده ارسال می‌کند که در این پروسه‌ی فشرده‌سازی تغییراتی به‌وجود می‌آید و امکان این نیز وجود دارد که بعضی از Requestها ازبین بروند و این روند تغییر Request ها نیاز به یک مدت زمان زیاد دارد و تمام این پروسه توسط RADIUS Accounting Server صورت می‌گیرد (۱۴). بناءً، سرورهای زیاد موجود می‌باشند که RADIUS Protocol و استندردهای آن را حمایت می‌کنند و بعضی از کاربرها مشخصه‌ها و پالیسی‌های خاص خود را در RADIUS Server تطبیق می‌نمایند (۱۵). هم‌چنان تحقیقات نشان داده که مشهورترین پروتکل برای وصل شدن به یک سرور بیرونی بعد از

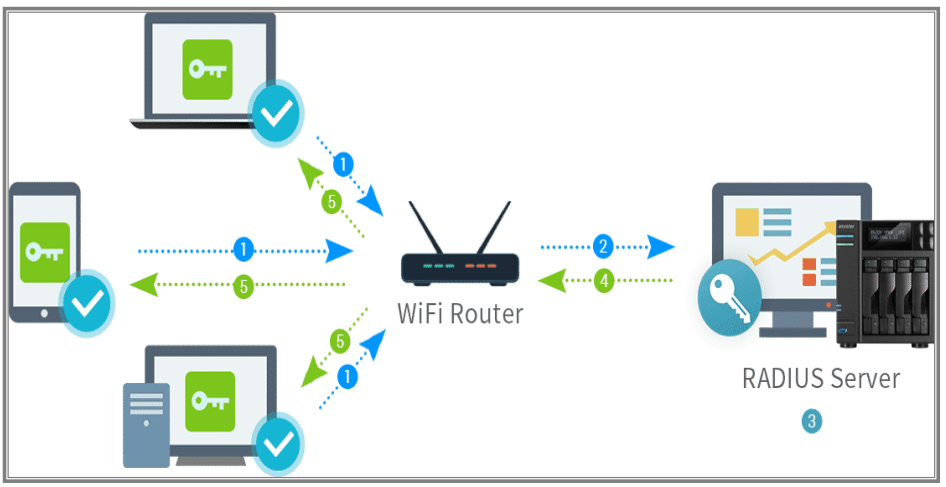
احراز هویت RADIUS می‌باشد و این احرازهویت بین Access Point و کاربر توسط RADIUS Server در شبکه‌ی بی‌سیم محلی صورت می‌گیرد (۵). سرور RADIUS سیستم‌ها را قادر می‌سازد تا از سه عدد سرور استفاده نمایید، یک سرور را به حیث اصلی و یک یا دو سرور دیگر را برای سرور پشتیبانی تا احراز هویت و حسابی را برای هر یک از سرور RADIUSها طراحی نمایید (۱۶). سرور RADIUS یک پروتکل برای ارتباط اطلاعات می‌باشد که مدیریت امنیت را در محیط‌های که از راه دور کنترل می‌گردد، ارائه می‌نماید (۱۷). سرور ریدیوس اجازه می‌دهد تا دست‌رسی به شبکه‌ی خود را مدیریت بهتر نمایید و اجازه می‌دهد تمام معلومات امنیتی شبکه‌ی خود را در یک دیتابیس مرکزی به‌جای پراکنده کردن آن در تمام بخش‌های شبکه‌ی خود ذخیره نمایید (۱۸). رحمان (۲۰۱۴) بیان می‌دارد که سرور RADIUS یک پروتکل AAA می‌باشد که معمولاً برای وسایل شبکه‌مانند روتر، سویچ و غیره استفاده می‌شود RADIUS یک لایه حفاظتی در مقابل نفوذکنندها را ارائه می‌کند (۱۴).

بناءً، در اخیر داریم که RADIUS مخفف (Remote Access Dial-In User Service) است و یک پروتکل برای انجام عملیات‌های مختلفی از جمله احراز هویت یا Authentication، تعیین حدود دست‌رسی یا Authorization و گزارش‌گیری از عملکرد کاربران یا Accounting استفاده می‌شود. این پروتکل در سیستم عامل‌های مختلفی که در دنیا وجود دارد با انواع و اقسام روش‌ها و با استفاده از نرم‌افزارهای مختلف قابل پیاده‌سازی می‌باشد؛ اما در ویندوزهای سرور شرکت مایکروسافت نیز با عنوان NPS یا Network Policy Services شناخته می‌شود و این سرویس را می‌توانید در ویندوزهای سرور ۲۰۰۸ به بالا مشاهده کنید (۲).

به‌طور مشخص اگر با در نظرداشت تحقیق‌های بالا که توسط محققین صورت گرفته است، به ابعاد موضوع بپردازیم، RADIUS Server به سروری گفته می‌شود که می‌تواند عملیات‌های AAA یا همان سه عملیاتی که اشاره شد را انجام دهد. در یک شرکت یا سازمانی که ده‌ها RAS Server یا Remote Access Server وجود دارد، منطقی نیست که همه عملیات‌های احراز هویت توسط سرورها انجام شود. در چنین حالتی برای متمرکزسازی این سه عملیات از NPS یا RADIUS Server استفاده می‌شود (۹) به تجهیزات یا سرویس‌های که می‌توانند عملیات احرازهویت خود را به گردن RADIUS Server بیندازند، در اصطلاح RADIUS Client گفته می‌شود که در ویندوزهای سرور موارد زیر را می‌توانیم به عنوان RADIUS Client داشته باشیم:

- Dial-Up Server
- Wireless Access Point
- VPN Server
- Router
- Switch

زمانی‌که از طرف RADIUS Client ها درخواستی برای NPS یا همان RADIUS Server ارسال می‌شود، این سرویس در واقع مرکز اصلی احراز هویت و تعیین حدود دسترسی به تمام درخواست‌های که از RADIUS Client ها ارسال شده ارائه می‌کند. سرویس NPS از دیتابیس Directory Active برای احراز هویت کاربران استفاده می‌کند که در شکل ۱ نشان‌داده شده است (۱۹).



شکل۱: نحوه‌ی کار سرور RADIUS با Access Point (6).

روش تحقیق

در این تحقیق روش آزمایشی مورد استفاده قرارگرفته است. بناءً، به اساس این روش نخست سرور RADIUS در روی سیستم عامل سرور ویندوز ۲۰۱۲ راه‌اندازی شده و بعد یک گروه از نام عبور و رمز را درین سیستم تعریف نموده و دسترسی استفادکنندگان که از طریق تکنالوژی Access Point با استفاده از پروتکل‌های امنیتی بی‌سیم (WPA و WPA2 Enterprise) که با سرور RADIUS هم‌خوانی دارند، وارد سیستم شده اند.

جمع‌آوری اطلاعات

آزمایش‌های کاربردی بالای استفادکنندگان از طریق سیستم عامل سرور ویندوز ۲۰۱۲ که دارای خدمات RADIUS می‌باشد و وسیله‌ی بی‌سیم Access Point صورت گرفته است. اطلاعات احراز هویت (Authentication)، تعیین حدود صلاحیت (Authorization)، گزارش‌گیری از عملکرد کاربران (Accounting)، کارکرد RADIUS به اساس نوعیت استفاده‌ی پروتکل‌های TCP و UDP و هم‌چنان عملکرد این سرور نظر به حمایت الگورتم‌های رمزگزاری و رمزگشایی مورد آزمایش قرارگرفته و اطلاعات به این شکل جمع‌آوری شده است.

تحلیل و تجزیه

پروسه‌ی احراز هویت و تعیین حدود صلاحیت توسط سرور RADUIS یک‌جا اجرا می‌شود و پروسه‌ی گزارش‌گیری از عملکرد کاربران به طور جداگانه صورت می‌گیرد. اما قابل یادآوری است که گزارش عملکرد کاربران (Accounting) درین سرور به‌خاطر سازگاری با سرور ثبت گزارش‌ها مانند (SysLog Server) و دیگر سرورها حایز اهمیت است. باید گفت که سرور RADIUS می‌تواند که تنها اطلاعات اسم عبور را رمزگزاری کند و هم‌چنان باید یادآور شد که سرویس گیرندگان RADIUS از طریق پورت‌های ۱۸۱۲ و ۱۸۱۳ پروتکل UDP با یک سرویس‌دهنده‌یRADIUS ارتباط برقرار می‌نمایند. سرویس‌گیرنده RADIUS می‌تواند یک سرویس‌دهنده‌ی دست‌یابی شبکه‌ی NAS، برگرفته شده از (Network Access Server) و یا هرنوع دستگاه مشابه دیگری باشد که نیازمند authentication و accounting است را احراز هویت کند. در کُل گفته می‌توان که این سرور نظر به استفاده‌ی گروه از کاربران تعریف شده در سیستم قابل انعطاف‌پذیری بیشتری را ایجاد می‌کند.

یافته‌های تحقیق

سرور RADIUS احراز هویت، تعیین حدود دسترسی و گزارش‌گیری از عملکرد کاربران را بین یک سرویس‌گیرنده‌ی RADIUS و یک سرویس‌دهنده‌ی RADIUS حمل می‌نماید. سرویس‌گیرنده‌ی RADIUS می‌تواند یک سرویس‌دهنده‌ی دست‌یابی شبکه NAS، برگرفته شده از (Access Server Network) و یا هرنوع دستگاه مشابه دیگری باشد که نیازمند authentication و accounting است. همان‌گونه که اشاره گردید NAS به عنوان یک سرویس‌گیرنده RADIUS عمل می‌نماید. سرویس‌گیرنده مسوول ارسال اطلاعات کاربر برای سرویس‌دهنده RADIUS است تا براساس نتایج برگردانده شده توسط سرویس‌دهنده، در مورد آن کاربر تصمیم گرفته شود. سرویس‌دهندگان RADIUS مسوول دریافت درخواست ارتباط کاربر، تأیید وی و ارسال اطلاعات مورد نیاز برای سرویس‌گیرنده به منظور عرضه‌ی سرویس به کاربر می‌باشند. یک سرویس‌دهنده RADIUS می‌تواند به عنوان یک سرویس‌گیرنده Proxy به سایر سرویس‌دهندگان RADIUSعمل نماید.

سرور RADIUS می‌تواند امنیت شبکه‌ی بی‌سیم محلی را تضمین کند، به این صورت که بعد از راه‌اندازی سرویس RADIUS بر روی ویندوز، سرور برای هر کاربر نام کاربری و رمز ورود تعریف می‌کند و هنگامی‌که یک کاربر بخواهد به شبکه‌ی بی‌سیم محلی وصل گردد، ضرور است تا نام کاربری و رمز ورود خاص خود را که در سیستم عامل موجود است، وارد نماید. بنابراین، سرور

RADIUS در شبکه‌های بی‌سیم از اهمیت خاص برخوردار می‌باشد، چون کابران مجاز با استفاده از پروتکل‌های امنیتی بی‌سیم محلی مانند WPA2 Enterprise از طریق Access Point به گروه از کاربران که در سیستم موجود است دسترسی پیدا کرده و از دسترسی اشخاص غیرقانونی به شبکه‌ی بی‌سیم جلوگیری می‌کند و یک سرویس مرکزی احراز هویت و تعیین حدود صلاحیت را فراهم می‌کند و به جای این‌که هر سرور به صورت جداگانه نیازمند یک دیتابیس باشد تا اشخاص را احراز هویت کند، درخواست‌های احراز هویت و تعیین حدود صلاحیت به یک سرور مرکزی ارسال می‌گردند. و تمام اطلاعات مهم یک شخص و یا یک کاربر در یک وسیله‌ی مرکزی حفظ و نگه‌داری می‌گردد.

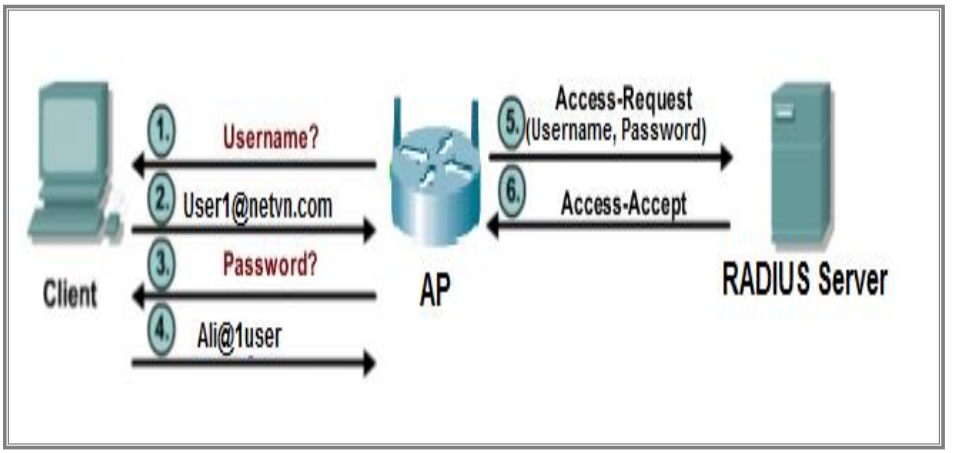
با استفاده از شبکه‌های کیبلی و یا بی‌سیم این اطلاعات در اسرع وقت به دسترس کاربران آن قرار می‌گیرد و سرور RADIUS از دست‌رسی افراد غیرمجاز به آن جلوگیری می‌کند.

در بحث RADIUS، منظور یک کاربر ساده که کاربر با آن کار می‌کند نیست، بلکه منظور از NAS های مانند Dial-up server، VPN server، Wireless access point و یا Proxy server بوده که چندین کاربر معمولی (کاربر عادی) به آن‌ها متصل می‌شوند. تمام این سرورها به تنهایی، کار شناسایی هویت از کاربرها را انجام می‌دهند ولی با RADIUS server این کار متمرکز خواهد بود.

در سرور RADIUS عمل Authentication به معنای این‌ست که آیا کاربری که می‌خواهد به شبکه وصل گردد، جزء کاربرهای شما در active directory است یا خیر؟ حال اگر کاربر، شناسایی هویت شده و وارد شبکه شد، به چه منابع و در چه سطحی به آن‌ها دسترسی داشته باشد که توسط Authorization مشخص می‌شود. سپس Accounting مشخص می‌کند در چه زمان‌های کاربرها می‌توانند به چه میزانی از منابع دست‌رسی داشته باشند.

نتیجه‌گیری

با استفاده از سرور RADIUS تمام کاربران را که می‌خواهند به شبکه وصل گردند، می‌توان احراز هویت کرد و این سرور در شبکه‌های بی‌سیم محلی برای امنیت با یک سطح بالا یک نقطه‌ی مرکزی برای احراز هویت و تعیین حدود صلاحیت برای کابران را فراهم می‌نماید. بناءً، این سرور با داشتن انعطاف‌پذیری بیشتر، در سیستم‌های مختلف مورد استفاده قرار می‌گیرد. در شکل ۲ چگونگی نحوه‌ی کارکرد این سرور با یک کلاینت را مشاهده می‌کنید.



شکل۲: کارکرد سرور RADIUS با کلاینت (۴)

مطابق به شکل۲ فوق اگر معلومات امنیتی برای احراز هویت نادرست باشد، به شبکه‌ی بی‌سیم وصل نمی‌توان شد، اگر معلومات را درست وارد کرده باشید به شبکه وصل می‌شوید. بنابرین، باید گفت که RADIUS Server تمام وسایل شبکه‌ی بی‌سیم مثل Access Point ها را تحت اثر خود قرار داده یعنی وسایل بی‌سیم تمام پالیسی‌های امنیتی خود را از سرور مربوطه اخذ می‌نماید و زمانی‌که کاربرها توسط Access Point به شبکه وصل گردیدند می‌توان با استفاده RADIUS Server آن‌ها را کنترل نمود.

این سرور عملکردهای مختلفی از جمله احرازهویت یا Authentication، تعیین حدود دست‌رسی یا Authorization و گزارش‌گیری از عملکرد کاربران یا Accounting را در یک نقطه مرکز فراهم نموده، انجام می‌دهد. در شبکه‌ی بی‌سیم RADIUS Server نخست کاربرها را با استفاده از اسم عبور و رمز عبور که در دومین ثبت گردیده است، شناسایی نموده و از طریق سرور به آن‌ها می‌توان پالیسی‌ها را اعمال کرد، و از عملکرد آن‌ها گزارش‌گیری نمود. لذا، نقش اساسی سرور RADIUS در شبکه‌های بی‌سیم محلی این است که بجای این‌که تکنالوژی‌ها و وسایل به‌صورت جداگانه هرکدام شان کاربران را احراز هویت نمایند، این کار توسط یک نقطه‌ی مرکزی صورت می‌گیرد و بالای اطلاعات انواع مختلف پروتکول‌های رمزگذاری مانند WEP, WPA, WPA2 را در پروسه‌ی احراز هویت توسط این سرور استفاده کرده می‌توانیم.

در اخیر باید گفت که زمانی‌که در دومین برای هر کاربر یک User ایجاد کرد و می‌توان تعدادی از کاربرها را عضو یک گروپ مشخص ساخت، بعداً بالای آن‌ها پالیسی اعمال کرد و لازم است تا تمام گروپ‌ها را در زمان عیارسازی NPS مشخص نماییم.

منابع

(1) R.Egli P. AAA / RADIUS REMOTE AUTHENTICATION. 2015, pp.1-12.

(2) Pratap A, Saxena P. An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS+. Int J Comput Appl. 2017;169(9), pp. 6-10.

(3) Kumkar V, Tiwari A, Tiwari P, Gupta A, Shrawne S. Vulnerabilities of Wireless Security protocols (WEP and WPA2). Int J Adv Res Comput Eng Technol. 2012; 1(2), pp. 2278-1323.

(4) Vinay Kumar SB, Prasanna Kumar C, Shahi B, Jha D, Monica B V., Suresh Kumar CP. Role of Diameter Based Protocol in enhancing of new and Upcoming Technologies. Phys Procedia. 2016; 78, pp. 415-22.

(5) Garais G. Cost Effective RADIUS Authentication for Wireless Clients. Database Syst J. 2010; 1(2), pp. 27-32.

(6) Zou Y, Zhu J, Wang X, Hanzo L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proc IEEE. 2016;104(9), pp. 1727-65.

(7) Fonseca J, Seixas N, Vieira M, Madeira H. A Survey on Wireless Security Protocols (WEP, WPA and WPA2. IEEE Trans Dependable Secur Comput. 2014;11(2), p. 4.

(8) Dmitry O. RADIUS server as centralized authentication. 2015.

(9) Ravi V, Sunitha NR, Pradeep R, Verma S. Formal methods to verify authentication in TACACS+ protocol. 2017 2nd Int Conf Emerg Comput Inf Technol ICECIT 2017. 2018, pp. 1-4.

(10) Chhabra N. Comparative Analysis of Diferent Wireless Technologies. 2013,1(5).

(11) Differences P. The Advantages of TACACS + for Administrator Authentication. 2011, pp. 1-6.

(12) Deshmukh R V. Flapping RADIUS accounting server behavior with toggle-timer. Proc - 2012 7th Int Conf Broadband, Wirel Comput Commun Appl BWCCA 2012. 2012, pp. 558-61.

(13) Barhoom TSM. Implementation and Comparison of OTP Techniques (TOTP,HOTP,CROTP) to Prevent Replay Attack in RADIUS Protocol. 2014.

(14) Rehman MH, Govardhan DA, Narayana Rao TV. Design and Implementation of RADIUS–An Network Security Protocol GJCST Computing Classification. 2014;10(October 2014), pp. 48-54.

(15) Mishra Y, Marwah GK, Verma S. Arduino Based Smart RFID Security and Attendance System with Audio Acknowledgement. 2015;4(01), pp. 363-7.

(16) Keski-kasari S, Huhtanen K, Harju J. Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET). pp. 1-11.

(17) Zhou J, Yan Y, Wang L, Guo Y. Comparative Analysis and Application of Common Authentication and Accounting Technology in the Modern Network. www.ijape.org Int J Autom Power Eng. 2013;2(4), pp. 84-9.

(18) Paramitha AP, Rochim AF, Fauzi A. Design and Implementation Network Administrators Account Management System Based on Authentication, Authorization, and Accounting Based on TACACS and LDAP. IOP Conf Ser Mater Sci Eng. 2020; 803(1).

(19) Weissman D, Jayasumana A. Integrating IoT Monitoring for Security Operation Center. In: GIoTS 2020 - Global Internet of Things Summit, Proceedings. 2020.