# آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 58)


در شماره گذشته آموزش نتورک‌پلاس با مباحث تایید هویت محلی، تعیین سطح دسترسی، کنترل دسترسی به شبکه، توپولوژی‌های کنترل دسترسی، حسابرسی، راه‌حل‌های کنترل دسترسی به شبکه، توپولوژی‌های کنترل دسترسی و سرویس‌های دایرکتوری آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

**رای مطالعه بخش پنجاه و هفتم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید**

همان‌گونه که در شماره‌های گذشته به آن اشاره داشتیم برای درک دقیق اینکه چگونه یک کلاینت از Kerberos استفاده می‌کند، باید با یکسری اصطلاحات مرتبط با این فناوری آشنا شوید.

• principal- یک کلاینت یا کاربر Kerberos است.

• KDC سرنام Key Distribution Center- سروری است که در زمان تأیید هویت اولیه کلاینت‌ها کلیدها را به آن‌ها تخصیص می‌دهد.

• ticket - یک مجموعه موقتی از اعتبارنامه‌هایی است که یک کلاینت برای اثبات هویت خود به سرورهایی که نیازمند دسترسی به آن‌ها است ارائه می‌کند.

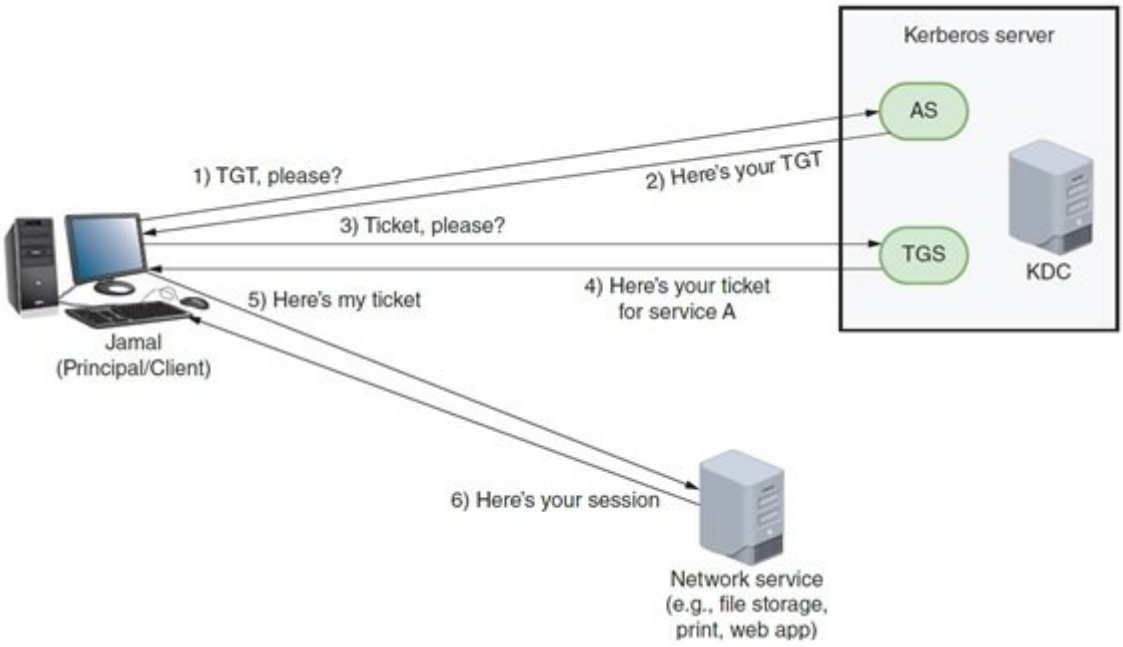
یک سرور Kerberos دو سرویس زیر را اجرا می‌کند:

• AS سرنام authentication service - سرویس تأیید هویت بوده که یک اعتبارسنجی اولیه را روی یک کلاینت انجام می‌دهد.

• TGS سرنام ticket-granting service- مجوزی را به یک کلاینت احراز هویت شده برای دسترسی به خدمات شبکه ارائه می‌کند

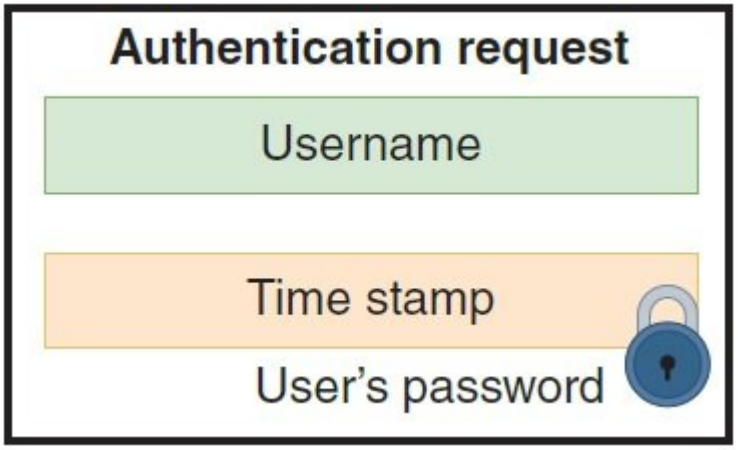
اکنون که با اصطلاحات اساسی Kerberos آشنا شدید، زمان آن فرا رسیده است تا با فرآیند پردازش دسترسی و ارتباط کلاینت-سرور آشنا شوید. در نظر داشته باشید که هدف Kerberos برقراری ارتباط یک کاربر احراز هویت شده با سرویسی است که کاربر قصد دسترسی به آن‌را دارد. دسترسی به ایمیل، چاپ، فایل سرور، بانک‌اطلاعاتی یا برنامه‌های وب از جمله این موارد است. برای انجام این کار، کاربر و سرویس باید پیش از این اطلاعات‌شان در AS

ثبت شده باشد و کلیدهای مخصوص خود را داشته باشند. شکل زیر نشان می‌دهد که TGS چگونه کار می‌کند.

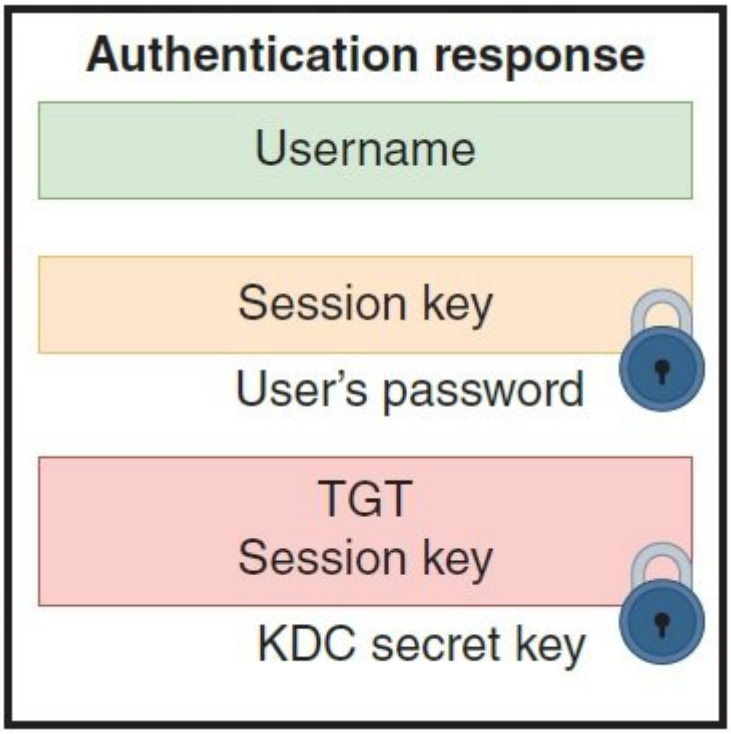



فرآیند احراز هویت با Kerberos به شرح زیر است:

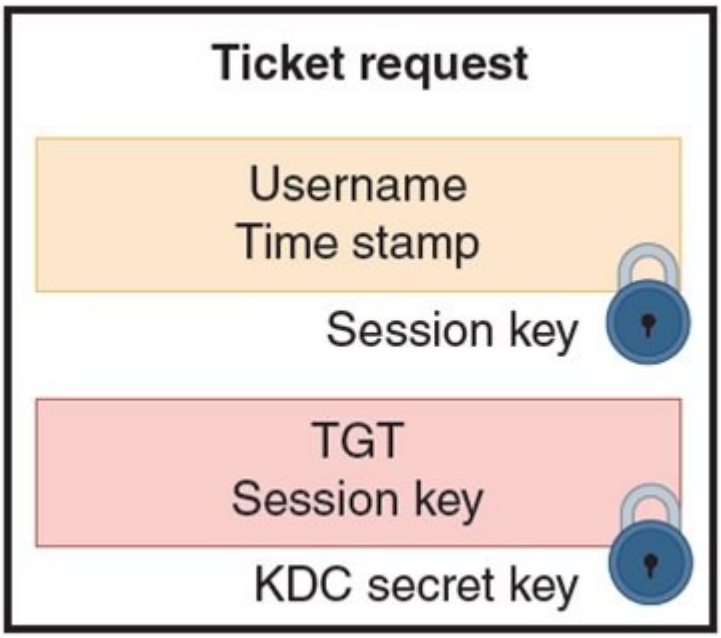
مرحله 1: هنگامی که کاربر (جمال در مثال ما) برای اولین بار وارد شبکه می‌شود، کامپیوترش یک درخواست احراز هویت را به AS ارسال می‌کند. این درخواست شامل نام کاربری Jamal اما گذرواژه او نیست. با این حال، مهر زمانی روی درخواست با گذرواژه جمال رمزگذاری شده است.



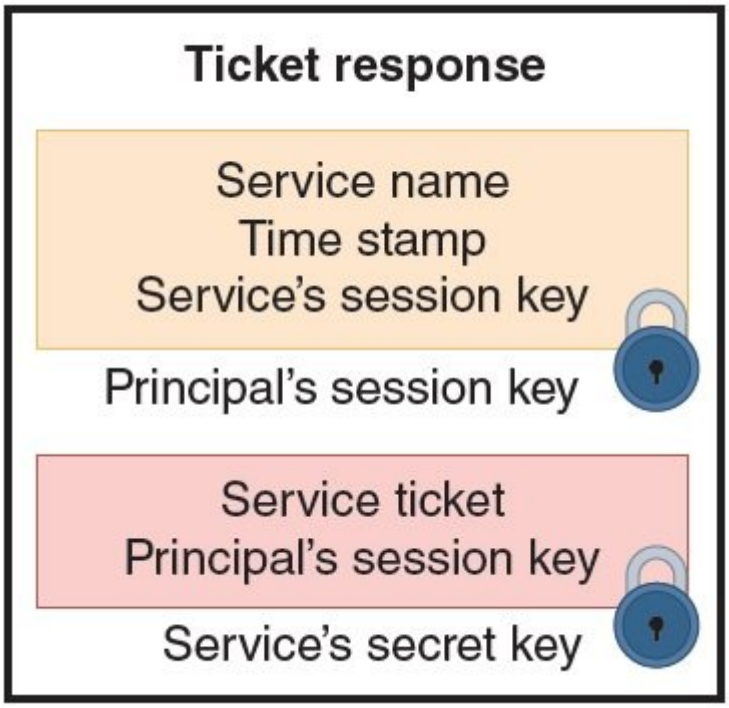

مرحله 2: AS در KDC برای اولین بار تایید می‌کند که اطلاعات جمال در پایگاه داده‌اش وجود دارد و از گذرواژه خود (بازیابی شده از پایگاه داده خود) برای رمزگشایی مهر زمانی استفاده می‌کند. اگر مشکلی وجود نداشته باشد، AS یک کلید نشست را ایجاد می‌کند که برای رمزگذاری و رمزگشایی ارتباط در آینده استفاده می‌شود. این کلید در ادامه با گذرواژه کاربر رمزگذاری می‌شود. AS همچنینTGT سرنام Ticket-Granting Ticket را تولید می‌کند که در یک بازه زمانی مشخص (به‌طور پیش‌فرض 10 ساعت ) منقضی می‌شود. برای جلوگیری از جعل و تقلب، TGT با یک کلید مخفی KDC رمزگذاری می‌شود. دقت کنید که تنها KDC می‌تواند کلید مخفی را خوانده و صحت آن‌را تأیید کند.



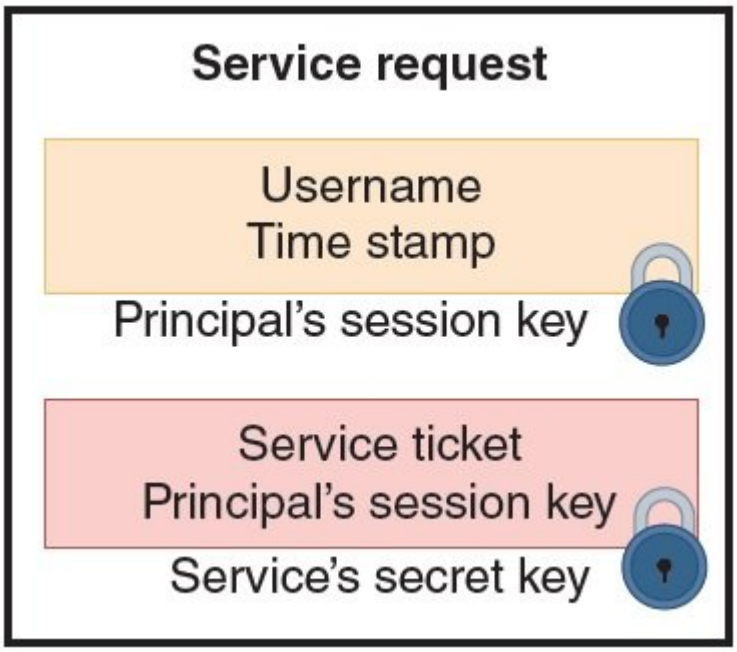

مرحله سوم پس از دریافت TGT، کاربر کلید جلسه را با استفاده از گذرواژه خود رمزگشایی می‌کند. اگر گذرواژه صحیح استفاده شده و رمزگشایی موفق باشد، کاربر می‌تواند یک درخواست بلیط را برای TGS و دسترسی به یک سرویس شبکه ارسال کند. این درخواست شامل نام کاربری و مهر زمانی است که هر دو با استفاده از کلید جلسه رمزگذاری می‌شوند. این درخواست همچنین شامل TGT کاملا رمزگذاری شده است که کاربر هیچ‌گاه آن‌را رمزگشایی نخواهد کرد.




گام چهارم، TGS به تایید اعتبار TGT و محتویات پیام درخواست پرداخته و سپس یک بلیط ایجاد می‌کند که کاربر (Jamal) را قادر می‌سازد از سرویس شبکه استفاده کند. این بلیط شامل نام سرویس، یک مهر زمانی و کلید نشست سرویس است که همه آنها با استفاده از کلید جلسه صادر شده در مرحله قبل رمزگذاری شده‌اند. این بخش با استفاده از یک کلید مخفی که سرویس از آن اطلاع دارد، رمزنگاری می‌شود. کاربر در ارتباط با این کلید اطلاعی ندارد.




گام پنجم، کامپیوتر جمال از کلید نشست برای رمزگشایی اطلاعاتی که به آن‌ها نیاز دارد استفاده می‌کند. سپس یک درخواست برای دسترسی به سرویس موردنظر ایجاد می‌کند که حاوی اطلاعات رمزگذاری شده از TGS همراه با یک مهر زمانی است که با کلید جلسه رمزگذاری شده‌اند.




گام ششم، سرویس بلیط را با استفاده از کلید مخفی خود، رمزگشایی می‌کند، کلید جلسه اصلی کاربر که شامل بلیط است را پیدا می‌کند و سپس مابقی پیام را رمزگشایی می‌کند تا اعتبار آن‌را تأیید کند. در نهایت، سرویس تأیید می‌کند کاربری که درخواست استفاده از سرویس را ارائه کرده در سرور KDC ثبت شده و اجازه دسترسی را می‌دهد.

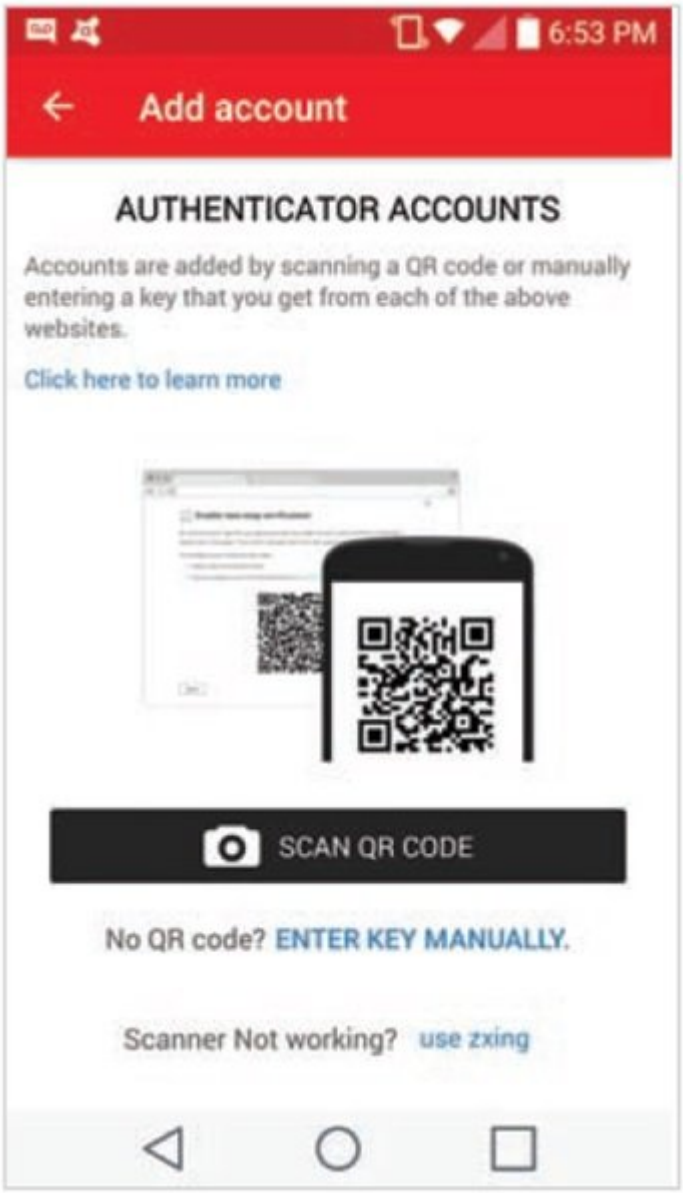
**نکته**: Kerberos از سوی موسسه تحقیقاتی MIT طراحی شده است. اما تولیدکنندگان نرم‌افزارهای مختلف نسخه‌های خاص خود را از این فناوری توسعه داده و استفاده می‌کنند.

## احراز هویت و ورود یکپارچه با رویکرد Single Sign-On

Kerberos مثالی از SSO سرنام Single Sign-On است. یک شکل احراز هویت است که در آن کلاینت با یک بار ورود به سیستم‌ها یا منابع مختلف دسترسی خواهد داشت. مزیت اصلی ورود یکباره به سیستم تنها راحتی است. کاربران مجبور نیستند چندین گذرواژه را حفظ کنند و مدیران شبکه می‌توانند مدت زمان کمتری صرف مدیریت گذرواژه‌ها کنند. اما بزرگ‌ترین عیب این روش به نحوه دسترسی به منابع باز می‌گردد، زیرا کاربر تنها با یکبار احراز هویت قادر است به همه بخش‌های شبکه دسترسی داشته باشد. بهترین مثالی که در ارتباط با فناوری SSO می‌توان به آن اشاره کرد گوگل است. زمانی که شما یکبار به یکی از حساب‌های کاربری خود وارد شوید، در ادامه قادر هستید به همه سرویس‌های دیگر گوگل نیز دسترسی داشته باشید. در نقطه مقابل یک هکر با کمی صرف وقت و به دست آورند گواهی‌نامه‌های (محدود) مربوطه قادر است به بیشتر فایل‌ها و ارتباطات درون شبکه دسترسی پیدا کند. برای افزایش بیشتر امنیت، برخی از سیستم‌ها، نسخه خاصی از SSO را استفاده می‌کنند که در آن کلاینت‌ها را مجبور می‌کنند دو یا چند قطعه از اطلاعات خاص را برای تأیید هویت خود ارائه کنند. در یک سناریوی احراز هویت دو مرحله‌ای **2FA** سرنام **two-factor authentication**، کاربر باید چیزی را ارائه کند تا چیزی را به دست آورد. به‌طور مثال، کاربر ممکن است یک اسکن اثر انگشت را در کنار گذرواژه خود به سیستم ارائه کند. یک فرآیند احراز هویت که به دو یا چند قسمت از اطلاعات نیاز دارد، به عنوان احراز هویت چند عاملی **MFA** سرنام **multifactor authentication** شناخته می‌شود. در **آزمون نتورک‌پلاس** شما باید با پنج فاکتور احراز هویت آشنا باشید. این فاکتورها همراه با مثال‌های آن‌ها به شرح زیر هستند:

- چیزی که می‌دانید - گذرواژه، پین‌کد یا داده‌های زیستی
- چیزی که دارید - کارت ATM، کارت هوشمند یا کلید
- چیزی که شما هستید - اثر انگشت، الگوی چهره یا الگوی عنبیه
- جایی که هستید - مکان شما در یک ساختمان خاص یا اتاق امن
- چیزی که انجام می‌دهید - روش خاصی است که تایپ می‌کنید، صحبت می‌کنید یا راه می‌روید.

احراز هویت چند عاملی حداقل به دو مورد از روش‌هایی که به آن‌ها اشاره شد نیاز دارد. به‌طور مثال، ورود به شبکه ممکن است به یک گذرواژه، اسکن اثرانگشت و همچنین اطلاعاتی که توسط یک نشانگر امنیتی تولید شده است نیاز داشته باشد. یک **نشانه امنیتی** (**security token**) یک دستگاه یا برنامه‌ای است که اطلاعات را ذخیره یا تولید می‌کند. یک سری از اعداد یا حروف که تنها کاربر مجاز از وجود آن‌ها اطلاع دارد از جمله این موارد است. در شکل زیر یک برنامه گوشی هوشمند را مشاهده می‌کنید که درخواست یک کد QR را ارائه کرده است که این کد توسط یک وب‌سایت برای ایجاد یک حساب کاربری تولید می‌شود.



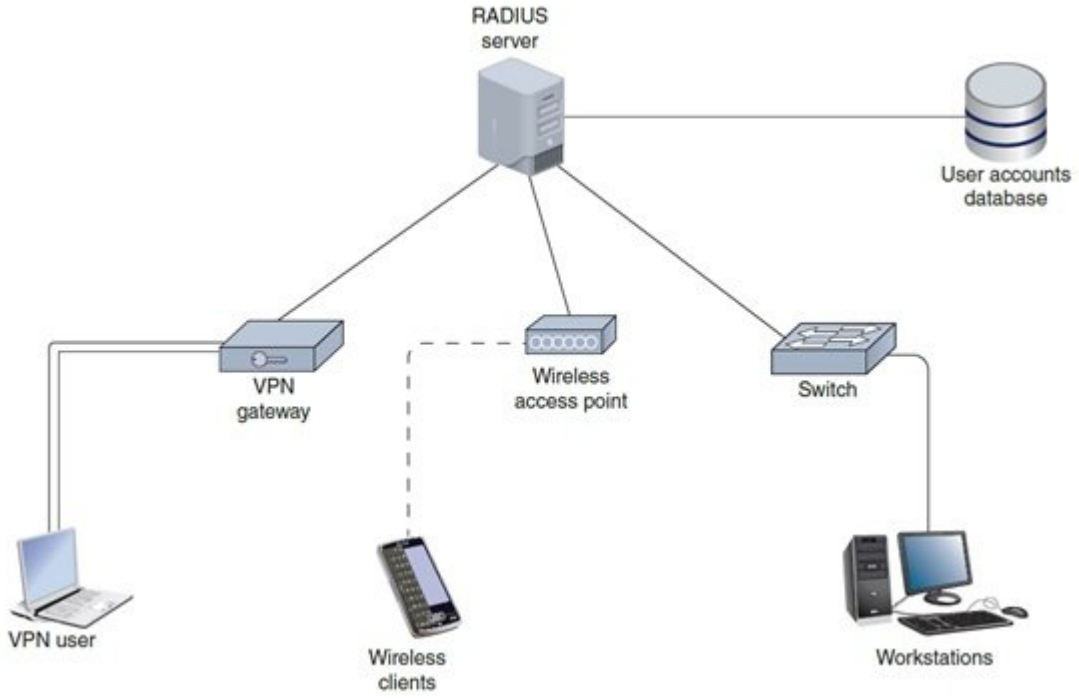

این کد تصادفی عمد محدودی دارد و مدت زمان مشخص و محدودی همراه با گذرواژه کاربر برای دسترسی به حساب کاربری باید استفاده شود. در بعد سخت‌افزاری نیز می‌توان به نشانگر سخت‌افزار SecurID Jey chain fob اشاره کرد.


دستگاه **SecurID** یک گذرواژه ایجاد می‌کند که هر 60 ثانیه تغییر می‌کند. هنگام ورود به سیستم، کاربر باید شماره‌ای که دستگاه SecurID تولید کرده است را وارد کند. کاربر برای آن‌که بتواند به منابع امن شبکه دسترسی داشته باشد، ابتدا باید هویت خود را از طریق ارسال کدی که دستگاه برای او صادر کرد است به اثبات برساند.

Google Authenticator متعلق به گوگل نیز یک سرویس تولید کننده یک چنین کدی است که در اصل یک نرم‌افزار رایگان تولید کننده نشانه‌گرهای امنیتی است.

## Remote Authentication Dial-In User Service

محیط‌هایی که حجم بالایی از ارتباطات و چند شناسه هویتی و گذرواژه‌های مختلف کاربران را پشتیبانی می‌کنند به دنبال آن هستند تا از یک سرویس متمرکز برای مدیریت دسترسی بر پایه چارچوب AAA استفاده کنند. محبوب‌ترین سرویسی که در این زمینه وجود دارد خدمت احراز هویت کاربر از دور (**RADIUS**) سرنام **Remote Authentication Dial-In User Service** است. RADIUS یک استاندارد منبع باز است که توسط Livingston Enterprises در سال 1991 ایجاد شد و بعد از آن توسط سازمان IETF جامعیت پیدا کرد. استاندارد فوق در لایه کاربرد اجرا شده و می‌تواند از هر دو پروتکل UDP یا TCP در لایه انتقال استفاده کند. رادیوس دو رویکرد احراز هویت و تعیین سطح دسترسی را در قالب یک فرآیند واحد بررسی می‌کند، به این معنا که یک بسته یکسان برای هر دو فرآیند استفاده می‌شود، در حالی که حسابرسی به عنوان یک فرآیند جداگانه انجام می‌شود. رادیوس می‌تواند به عنوان یک برنامه نرم‌افزاری روی یک سرور دسترسی از راه دور یا روی کامپیوتری که برای این نوع احراز هویت در نظر گرفته شده و به آن سرور رادیوس (RADIUS server) می‌گویند استفاده شود.




از آنجایی که سرورهای RADIUS گسترش‌پذیری بالایی دارند، بیشتر ISPها از یک سرور RADIUS به عنوان یک نقطه مرکزی برای احراز هویت کاربران بی‌سیم، همراه و راه دور استفاده می‌کنند. خدمات رادیوس اغلب با سایر سرویس‌های شبکه روی یک ماشین انفرادی ترکیب می‌شوند. به‌طور مثال، یک سازمان ممکن است یک سرور DHCP را با یک سرور RADIUS ترکیب کند تا تخصیص آدرس‌ها و امتیازات اختصاص داده شده به هر آدرس در شبکه به بهترین شکل مدیریت شوند. شکل زیر یک سرور RADIUS که فرآیند دسترسی به شبکه را برای کاربران راه دور و محلی مدیریت می‌کند را نشان می‌دهد.. RADIUS می‌تواند تقریبا در تمام سیستم‌عامل‌های مدرن اجرا شود. در حالی که RADIUS شامل برخی از ویژگی‌های بسیار پیچیده حسابرسی است، اما گذرواژه‌ها را تنها در زمان انتقال رمزگذاری می‌کند و بنابراین به عنوان TACACS+ امن که در ادامه با آن آشنا خواهید شد در نظر گرفته نمی‌شود.

## Terminal Access Controller Access Control System Plus

کنترل کننده دسترسي ترمینال و سیستم کنترل دسترسي TACACS+ سرنام Terminal Access Controller Access Control System Plus، یکی دیگر از پروتکل‌های محبوب AAA است که گزینه جداسازی احراز هویت، تعیین سطح و قابلیت‌های حسابرسی را در اختیار مدیران شبکه قرار می‌دهد. به‌طور مثال، TACACS+ ممکن است قابلیت‌های دسترسی و حسابرسی را فراهم کند، اما از تکنیک‌های مختلفی همچون Kerberos برای تأیید هویت

کاربران استفاده کند. TACACS+ متفاوت از RADIUS است به دلیل این‌که

• روی TCP و نه UDP در لایه انتقال مستقر می‌شود

• توسط سیسکو سیستمز برای استفاده‌های اختصاصی توسعه یافته است.

• به‌طور معمول روی یک روتر یا سوئیچ و نه روی یک سرور نصب می‌شود.

• همه اطلاعات منتقل شده برای AAA را رمزگذاری می‌کند (RADIUS فقط گذرواژه را رمزگذاری می‌کند).

شما درباره چارچوب AAA و عملکرد آن روی یک شبکه و کنترل دسترسی کاربران به منابع شبکه مطالب بسیاری را آموختید. با این حال، هنگام تأیید اعتبار از طریق ارتباطات بی‌سیم باید ملاحظات خاصی در نظر گرفته شود. ارتباطات فوق کمتر کنترل شده و در برابر حملات MitM، جعل و سایر اکسپلویت‌ها آسیب‌پذیر هستند. اجازه دهید به‌طو خلاصه به این مسائل نگاهی داشته باشیم.

## امنیت شبکه بی‌سیم

در بخش شبکه‌های بی‌سیم، به‌طور خلاصه نیم نگاهی به امنیت شبکه‌های بی‌سیم داشتیم. به احتمال زیاد تاکنون مطالب بسیاری درباره آسیب‌پذیر بودن استاندارد WEP شنیده‌اید. آسیب‌پذیری‌هایی که در نهایت باعث شدند به ترتیب استانداردهای WPA، WPA2 و WPA3 به میدان وارد شوند. اکنون که اطلاعات بیشتری درباره رمزگذاری و احراز هویت یاد گرفته‌اید، آماده هستید تا درباره امنیت شبکه‌های بیسیم اطلاعات بیشتر به دست آورید. یکی از معایب بزرگ استاندارد WEP به‌اشتراک‌گذاری کلید رمزگذاری میان همه کلاینت‌ها باز می گردد، کلیدی که شاید هیچ‌گاه تغییر پیدا نکند. در حقیقت، WEP دو نوع احراز هویت که هیچ‌یک ایمن نیستند را ارائه می‌کند:

• **سیستم احراز هویت باز** (OSA) سرنام Open Authentication System - هیچ کلیدی استفاده نمی‌شود. یک کلاینت بی‌سیم با اطلاع از SSID یک اکسس‌پوینت یک درخواست احراز هویت ارائه می‌کند. AP یک کد تک نفره برای آن نشست تولید می‌کند و کامپیوتر آن کد را قبول می‌کند. با این حال، داده‌ها در این ارتباط موقت و در زمان ارسال هیچ‌گاه رمزگذاری نمی‌شوند و هر دستگاهی می‌تواند تایید اعتبار شود. در واقع هیچ احراز هویت واقعی رخ نمی‌دهد.

• **احراز هویت با کلید اشتراکی** (SKA) سرنام Shared Key Authentication - همه کلاینت‌های خواهان دسترسی بی‌سیم از کلید یکسانی استفاده می‌کنند که می‌تواند برای انتقال رمزگذاری شده استفاده شود. با این حال، کلید می‌تواند شکسته شده و امنیت همه کلاینت‌ها روی شبکه با خطر روبرو شود. با توجه به این ناامنی ذاتی، IEEE یک استاندارد جدید امنیت بی‌سیم به نام 802.11i را معرفی کرد. این استاندارد شامل استاندارد WPA بود که بعدها با WPA2 جایگزین شد.

در شماره آینده آموزش **نتورک‌پلاس** مبحث فوق را ادامه خواهیم داد.

**تاریخ انتشار:**
13 خرداد 1398

---

**نشانی منبع:**
https://www.shabakeh-mag.com/networking-technology/15487/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-58