در دنیاي امنیت داده ها اصطلاح پرکاربردی به نام AAA یا A3 وجود دارد که مخفف سه پروسه ی Authentication (بر اساس آن پروسه ها هویت حقیقی یا حقوقی کاربران خود را اثبات می کنند) Authorization (براساس آن تعیین می گردد کاربري که هویت او احراز شده، مجوز انجام چه کارهایی را دارد) Accounting (تشخیص می دهد پروسه یا کاربر چه سهمی از منابع سیستمی و خدمات را در اختیار خواهد داشت و آیا در ازاي دریافت آن، بهایی را پرداخت کرده است) می باشد، مهم ترین و اولین بخش از عملیات AAA همان عملیات احراز هویت می باشد. به همین دلیل ما در این بخش صرفا بر روی موضوع احراز هویت تمرکز خواهیم داشت.

Authentication یا احراز هویت به فرآیندی گفته می شود که در آن ارسال کننده یا دریافت کننده داده ها برای همدیگر اطلاعاتی را ارائه می کنند تا مطمئن شوند آنها همانی هستند که ادعا می کنند یا یک نفوذ گری که خود را به جای طرف واقعی جا زده است. این فرآیند می تواند بسیار ساده باشد، اما در شرایطی که می خواهید یک ارتباط راه دور را با احتمال وجود نفوذگران بسیار را برقرار کنیم، می تواند خیلی پیچیده و دشوار باشد و امن سازی چنین ارتباطاتی به پروتکلهای پیچیده ی مبتنی بر رمزنگاری نیاز دارد.

همچنین برخی افراد احراز هویت یا Authentication را با صدور مجوز یا Authorization اشتباه می گیرند ، حال اینکه در احرازهویت این سوال مطرح می گردد که شما واقعا در حال محاوره وتبادل اطلاعات هستید، درحالی که در صدور مجوز بررسی می گردد که هر پروسه مجوز انجام چه کارهایی را دارد و همچنین کاربرد واژه"احراز هویت" در مورد اشیایی مثل فایلها، برنامه هاي اجرایی و اسناد و مدارك، اشاره به پروسه ای دارد که بر اساس آن صحت و درستی آن شیء اثبات می گردد، اما در مورد افراد روشی براي تشخیص هویت واقعی آنان و اثبات درستی یا نادرستی ادعاي آنها در خصوص معرفی خودشان است.

برای حصول اطمینان از امنیت یک ارتباط طرفین از روشهای متعددی برای رمزگذاری داده ها و اطلاعات استفاده می کنند که می توان به روشهای ایجاد کلید های متقارن و نامتقارن اشاره نمود. درحین برقراری یک نشست به دلیل سرعت و کارآیی، داده هایی که در حین این نشست ردوبدل خواهند شد با کلید متقارنی که معمولا در آن از استاندارد های رمز نگاری AES یا DES استفاده می شود،رمزگذاری می گردند) .از رمزنگاری DESعموما برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود ، AESجانشین است که توسط آژانس امنیت ملی NSA برای اطلاعات فوق محرمانه پذیرفته شد (این الگوریتم‌ها تا زمانی که قرار است داده‌ها و رمز فقط نزد خود کاربر باشد و از آن استفاده کند، بهترین گزینه خواهد بود..

برای برقراری یک نشست امن بین دو طرف و تایید اصالت ودرستی آن نشست در طی سالهای گذشته پروتکلهای احراز هویت بسیاری ارائه گردید، در این پروتکلها برای ایجاد کلید نشست از روش رمز نگاری کلید عمومی در سطح گسترده ای استفاده می شود و در اکثر پروتکلهای احراز هویت طرفین یک نشست برای آن یک کلید سری یا به اصطلاح کلید خصوصی ایجاد می کردند تا در طی پروسه ی جاری از آن برای رمزنگاری استفاده نمایند.

فاکتورهای احراز هویت در حالت کلی به 4 دسته تقسیم میشوند:

فاکتور اول:چیزی که شما می دانید (What you know)

ساده ترین و البته ضعیف ترین مکانیزم احرازهویت یا Authentication در امنیت اطلاعات استفاده از یوزر (User Name)و پسورد (Password) است که اگر بخواهیم فارسی را پاس بداریم میشود نام کاربری و رمزعبور😊

مهمترین نکته ای که این مکانیزم دارد این است که اگر چیزی را که شما می دانید، شخص دیگری بداند پس آن شخص میتوان به جای شما احراز هویت شود. تجربه ما نشان داده بسیاری از افراد یوزر و پسورد خود را کنار سیستم یادداشت کرده اند و یا به راحتی نام کاربری و رمزعبور خود را در اختیار دیگران قرار می دهند و یا حتی پسورد های بسیار بسیار ساده را انتخاب می کنند که با نرم افزار های خاصی این گذرواژه ها قابل حدس زدن هستند که این امر باعث کاهش امنیت در سازمان شما خواهد شد.

فاکتور دوم:چیزی که شما دارید (What you have)

چیزی که شما دارید به این معناست که شما داری یک دستگاه فیزیکی هستید که این دستگاه شما را احراز هویت می کند و نیازی به این نیست که چیزی را به خاطر بسپارید. نقطه قوت این دستگاه همین است که از حفظ از کردن پسورد های متعدد بی نیاز می شوید ولی نقطه ضعفی هم دارد.

این را در نظر بگیرید که اگر در جای حساسی کار می کنید مثل یک دیتا سنتر کافیست این دستگاه به دست شخصی بیافتد که بخواهد سواستفاده کند و یا حتی به تاسیسات آن محل لطمه ای بزند که خب این کار به نام شما تمام خواهد شد.

انواع این دستگاه های فیزیکی مثل توکن های امنیتی یا کارت های هوشمند و ... می باشد.کارت های هوشمند همانند کارت هایی است که در بالا توضیح دادیم که البته مکانیزم ساخت و طراحی اش متفاوت تر است.

فاکتور سوم:چیزی که شما هستید (What you are)

کاربران ممکن است رمز عبور خود را فراموش کنند ، کاربران ممکن است کارت هوشمند خود را گم کنند اما قطعا فراموش نمی کنند که دست و بدن خود را همراه خود به این طرف و آن طرف ببرند😊 . در فاکتور سوم احراز هویت از اعضا و پارامترهای فیزیکی بدن انسان برای احراز هویت استفاده می شود که برای هر فردی در دنیا منحصر به فرد است . برای مثال در این نوع از احراز هویت از الگوی اثر انگشت ، الگوی صدای شخص ، الگوی مردمک و عنبیه چشم ، الگوی کف دست ، الگوی DNA و ... استفاده می شود.

مشکلاتی که در استفاده از این روش احراز هویت وجود دارد این است که ممکن است ما مواردی **false positive** و مواردی **false negative** داشته باشیم که به معنی وجود اشتباهات در سیستم احراز هویت است ، البته این مشکل بستگی به مکانیزمی دارد که شما استفاده می کنید.

یکی دیگر از مشکلاتی که برای پیاده سازی احراز هویت با فاکتور سوم وجود دارد این است که هزینه پیاده سازی این نوع مکانیزم بسیار بسیار بیشتر از هزینه های سایر سیستم های احراز هویتی در سطح کلان می

باشد. تهیه دستگاه های اسکنر اعضای بدن و قیمت های آن بسیار می تواند بالا باشد و بر حسب درجه امنیتی محل مورد نظر از سیستم هال مختلفی می تواند استفاده شود ، به فاکتور چیزی که شما هستید در اصطلاح فنی تر احراز هویت بیومتریک یا Biometric هم گفته می شود.

فاکتور چهارم:کاری که شما می کنید (What you do)

کاری که شما می کنید یا **What you do** در واقع یک نوع احراز هویت بیومتریک است که جزو زیرمجموعه های فاکتور سوم به حساب می آید ، در این روش احراز هویت رفتارهایی که شما انجام می دهید تجزیه و تحلیل می شود و بر حسب آنها تشخیص داده می شود که شخص مورد نظر همانی است که ادعا می کند یا خیر ، یکی از مرسوم ترین روش هایی که در این خصوص استفاده می شود سرعت تایپ کردن پسورد شما است ، فرض کنید شما پسورد خود را در حالت عادی در عرض ۱۵ ثانیه وارد می کنید و سیستم در صورتیکه شما در بازه زمانی ۱۵ تا ۲۰ ثانیه پسورد خود را وارد کنید تشخیص می دهد که خود شما هستید ، حالا فرض کنید که سیستم تشخیص می دهد که شما پسورد را درست وارد کرده اید اما بر حسب عادتی که داشته اید نبوده است و پسورد حدود ۴۰ تا ۵۰ ثانیه طول کشیده است تا وارد شود ، حالا با اینکه پسورد درست است اما سیستم احراز هویت تشخیص می دهد که پسورد شما به سرقت رفته است و شخصی در حال خواندن و تایپ کردن پسورد است و به شخص مورد نظر اجازه Login نخواهد داد. البته احراز هویت به این روش چندان هم دقیق نیست و به همین دلیل بیشترین استفاده از این نوع مکانیزم های احراز هویتی در لابراتوارها است و در محیط واقعی چندان کاربردی ندارند.

احراز هویت چند فاکتوری (Multifactor Authentication)

همانطور که از نامش هم پیداست یعنی از چندین فاکتور احراز هویت در احراز هویت افراد استفاده شود. برای مثال شما کارت بانکی که دارید دارای سیستم احراز هویت Two Factor Authentication یا احراز هویت دو فاکتوره است چون هم از شما رمز عبور پرسیده می شود و هم اینکه باید کارت بانکی را داشته باشید. یا اینکه شما کارت شناسایی دارید که بعد از وارد کردن کارت شناسایی در دستگاه مربوطه باید اثر انگشت شما نیز تایید شود و ایندو با هم تشکیل یک سیستم احراز هویت را می دهد.

درادامه برخی از پروتکلهای احراز هویت را که در شبکه های ناامن مورد استفاده قرار می گیرند را معرفی خواهیم کرد:

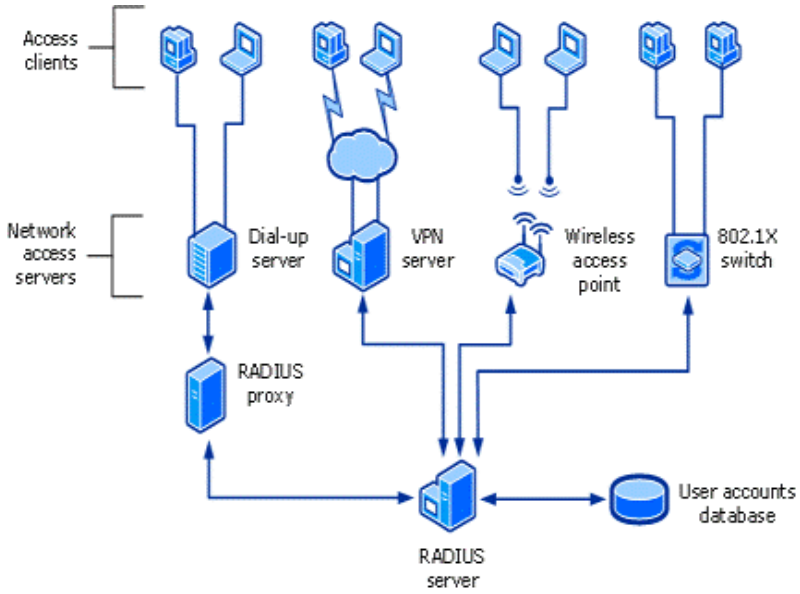
Kerberos

يك پروتكل امنيتي براي احراز هويت در شبكه است كه براي كاربران مجاز امكان ورود به شبكه پس از تاييد هويت را فراهم مي آورد. كاربران تيكت يا بليط هايي را از مركز توزيع كربروس (KDC) دريافت مي كنند. پس

از آن هنگامي كه ارتباط با شبكه فراهم شد كاربران اين بليط ها را به سرور ارائه مي كنند و در صورت تاييد، مجوز ورود به شبكه فراهم مي شود. بليط هاي كربروس اعتبار كاربران شبكه را نشان مي دهند.

RADIUS

این پروتکل به طور متمرکز وظایف AAA را برای کاربران هنگام دسترسی به سرویس ها و منابع شبکه انجام می دهد. مورد استفاده در مدیریت کاربران از راه دور (VPN Users) است.



احراز هویت براساس کلید مشترک و سری

در این پروتکل فرض می کنیم طرفین ارتباط قبلا در مورد یک کلید سری بنام K توافق کرده اند و این کلید سری را از طریق شبکه ی ناامن برای یکدیگر ارسال نکرده اند.

اساس کار این پروتکل بگونه ای است که یکی از طرفین با نام A بعنوان شروع کننده ی ارتباط مشخصه ی شناسایی خود را بدون رمزنگاری برای طرف مقابل یعنی B می فرستد تا او بتواند آن را بفهمد، در ادامه B عدد تصادفی بسیار بزرگ را بعنوان رشته ی چالش (nonce) برای طرف مقابل ارسال می کند و A نیزتبدیل خاصی را بوسیله ی کلید مشترک سری توافق شده بر روی آن عدد انجام می دهد و داده های رمز شده را به B بر می گرداند. به این ترتیب A متوجه می شود که این پیام واقعا از طرف B ارسال شده است زیرا هیچ کس از کلید مشترک بین آنها مطلع نبوده است.

برای اینکه طرف A هم از برقراری ارتباط با شخص درست اطمینان حاصل کند و بداند در این ارتباط شخص سومی در میان نیست عدد تصادفی دیگری را تولید و برای B ارسال می کند، در صورتی که B بتواند با استفاده از کلید مشترک پاسخ درست را برگرداند آنگاه A از سلامت ارتباط موجود مطمئن خواهد شد ودر این مرحله شروع کننده ی ارتباط کلید سری را برای نشست انتخاب کرده و آن را بوسیله کلید مشترک رمز کرده و برای طرف مقابل می فرستد. به چنین پروتکلهایی اصطلاحا پروتکلهای Challenge-Response

یا " چالش و پاسخ " می گویند. البته می توان مراحل این پروتکل را از 5 مرحله به 3 مرحله تقلیل داد و آن را کوتاهتر و سریعتر کرد.

متاسفانه پروتکلهای چالش و پاسخ با استفاده از تکنیکی به نام حمله ی بازتاب Reflection Attack شکسته شد.در این حمله نفرسوم با جستجو در شبکه و کپی کردن پاسخ های هر طرف و ارسال مجدد آن می توانست دیگری را فریب داده و در ارتباط اختلال ایجاد کند. البته اشکالات موجود در این پروتکل با ایجاد تغییراتی در قواعد آن برطرف شد.

مبادله ی کلید مشترک به روش دیفی- هلمن

در این روش فرض می کنیم طرفین ارتباط قبلا با یکدیگر ملاقات نکرده و در مورد یک کلید مشترک و سری هیچ توافقی نداشته اند. حال آنها باید حتی با آگاهی از وجود نفر سوم در ارتباط باز هم کلید مشترک و سری ایجاد کنند و انجام چنین عملی با پروتکل مبادله ی کلید دیفی-هلمن امکان پذیر خواهد بود.

احراز هویت توسط مرکز توزیع کلیدKDC

توافق و ایجاد یک کلید مشترک و سری با افرادی کاملا ناآشنا با روش بالا کاملا ممکن است اما دارای ایراداتی می باشد. مثلا در روش پیشین برای ایجاد ارتباط با تعداد زیادی از افراد به همان تعداد کلید سری نشست نیاز خواهید داشت و برای افراد عادی حفظ و مدیریت این همه کلید بسیار سخت است و جهت رفع چنین اشکالاتی راهکار متفاوتی بنام " مرکز توضیع کلید " یا KDC ارائه گردید.

در این روش هر کاربر تنها یک کلید دارد که بین او و مرکز توزیع KDC مشترک است و فرآیند احراز هویت و ایجاد کلید نشست از طریق KDC انجام می شود.فرض کنید برای برقراری ارتباط بین دو طرف A,B ابتدا طرف A که شروع کننده ی ارتباط خواهد بود یک کلید نشست سری را برای ارتباط خود با B انتخاب می کند و سپس تمایل ارتباط خود با طرف B را با استفاده از کلید نشست مشترک بین خود ومرکز توضیع رمز گذاری کرده و به KDC ارسال می کند، KDCپس از دریافت پیام آن را رمز گشایی کرده و مشخصه شناسایی طرف B و کلید سری نشست را از آن استخراج کرده و پیام جدیدی را ایجاد می کند که حاوی مشخصه ی شناسایی طرف A و کلید سری نشست خواهد بود و پیام جدید را با کلید سری مشترک بین خود وطرف B رمزگذاری کرده و پیام را برای B ارسال می کند.در ادامه B پس از دریافت پیام با استفاده از کلید سری مشترک بین خود و KDC پیام دریافتی را رمزگشایی کرده و درمی یابد که طرف A با استفاده از کلید نشست سری انتخاب شده خواهان برقراری نشست می باشد. در این روش احراز هویت بسیار ساده انجام می شود .

متاسفانه این پروتکل نیز با مشکل جدی مواجه شد. بدین ترتیب که شخص سوم با جستجو در شبکه می توانست پیغام های ارسال شده از طرف KDCکه حاوی مشخصه شناسایی و درخواست های طرف A است را کپی نموده و بارها آنها برای طرف B ارسال کند وطرف B نیز این درخواست را پذیرفته و آن را انجام دهد.این سری حملات به حمله ی تکرار یا "Replay Attack"معروف هستند.

چندین راه حل برای اینگونه حملات ارائه شد. اولین راه حل این بود که هر پیام دارای مهر زمان یا " Timestampباشد و در راه حل دوم توافق شد که هر پیام حاوی یک عدد یا رشته ی تصادفی باشد و

پیام هایی که دارای عدد یا رشته ی تکراری هستند، حذف شوند.هر دو این روش ها به تنهایی دارای کارآیی لازم نبوند اما استفاده از هر دو روش در پیام ها بطور همزمان می توانست موثرتر واقع شود.

راه حل پیچیده تری نیز برای آنکه طرفین بتوانند به کمک KDC یکدیگر را شناسایی کنند، ارائه شد که با استفاده از یک پروتکل چالش و پاسخ چند مرحله ای امنیت ارتباط ایجاد شده، تامین می گردید. از میان پروتکل های ارائه شده با این روش می توان از پروتکل احراز هویت نیدهام – شرودر نام برد .

احراز هویت با استفاده از رمز نگاری کلید عمومی

در این روش عملیات احراز هویت را می توان با استفاده از رمزنگاری با کلید عمومی انجام داد. برای انجام چنین روشی در شبکه به یک مرکز توزیع کلید عمومی به نام PKI با ساختار سرویس دهنده ی دایرکتوری نیاز داریم که بتواند Certificate های کلید عمومی را تحویل دهد.

برای شروع ارتباط بین دو طرف A,B طرف شروع کننده ی ارتباط مثلا A نیاز دارد که کلید عمومی B را از PKIدرخواست کند و در پاسخ PKI پیامی حاوی یک Certificate مثلا X.509 و کلید عمومی B را بازمی گرداند. پس از آنکه A صحت امضای B را بررسی و اطمینان حاصل کرد برای B پیامی که حاوی مشخصه ی شناسایی خود و یک nonce است را ایجاد کرده و پیام را با کلید عمومی B رمزگذاری کرده و برای طرف Bارسال می کند.

طرف B پس از دریافت پیام نمی داند که آیا واقعا پیام از طرف A فرستاده شده و یا شخص سومی این پیام را ارسال کرده است بنابراین به روش قبلی از PKI کلید عمومی طرف Aرا درخواست می کند و پس از دریافت پاسخ یک کلید سری نشست را انتخاب کرده و خود یک عدد تصادفی جدید ایجاد می کند و این دو را بهمراه عدد تصادفی دریافتی از A در قالب یک پیام جدید برای A آماده وآن را با کلید عمومی A رمز گذاری کرده و برای او ارسال می کند.

طرف A پس از دیدن عدد تصادفی تولید شده توسط خودش در پیام اطمینان حاصل می کند که طرف محاوره واقعا B می باشد و درمی یابد که این پیام تکراری نیست. بار دیگر A پیامی برای B می فرستد و در آن عدد تصادفی ایجاد شده توسط B را قرار داده و به وسیله کلید سری نشست پیشنهادی خود B رمزگذاری می کند و به این طریق توافق خود را در مورد کلید سری نشست پیشنهادی اعلام می کند.به این ترتیب B متوجه می شود که A عدد تصادفی که توسط او تولید شده بود را بررسی کرده است.

با استفاده از روش احراز هویت با استفاده از رمز نگاری کلید عمومی هیچ شخص سومی قادر به نفوذ در ارتباط انجام شده نخواهد بود.