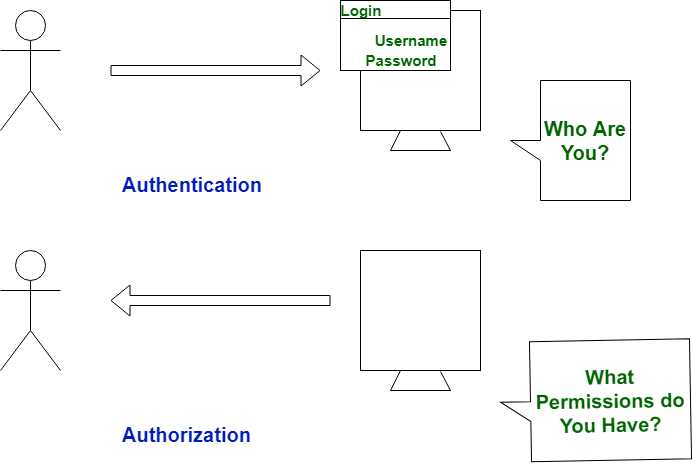
authentication and authorization



Authentication

المصادقة (AuthN) هي عملية تتحقق من أن شخصًا ما أو شيئًا ما هو ما يقوله. تستخدم أنظمة التكنولوجيا عادةً شكلاً من أشكال المصادقة لتأمين الوصول إلى التطبيق أو بياناته. على سبيل المثال، عندما تحتاج إلى الوصول إلى موقع أو خدمة عبر الإنترنت، يتعين عليك عادةً إدخال اسم المستخدم وكلمة المرور الخاصين بك. ثم، خلف الكواليس، يقوم بمقارنة اسم المستخدم وكلمة المرور اللذين أدخلتهما مع السجل الموجود في قاعدة البيانات الخاصة به. إذا كانت المعلومات التي قدمتها متطابقة، فإن النظام يفترض أنك مستخدم صالح ويمنحك حق الوصول. تفترض مصادقة النظام في هذا المثال أنك وحدك من يعرف اسم المستخدم وكلمة المرور الصحيحين. ومن ثم، فإنه يقوم بمصادقتك باستخدام مبدأ شيء لا يعرفه أحد سواك.

ما هو الغرض من المصادقة؟

الغرض من المصادقة هو التحقق من أن شخصًا ما أو شيء ما هو من أو ما يدعي أنه هو. هناك العديد من أشكال المصادقة. على سبيل المثال، لدى عالم الفن عمليات ومؤسسات تؤكد أن اللوحة أو النحت هو عمل فنان معين. وبالمثل، تستخدم الحكومات تقنيات مصادقة مختلفة لحماية عملاتها من التزييف. عادةً ما تحمي المصادقة العناصر ذات القيمة، وفي عصر المعلومات، تحمي الأنظمة والبيانات.

ما هو التحقق من الهوية؟

مصادقة الهوية هي عملية التحقق من هوية المستخدم أو الخدمة. وبناءً على هذه المعلومات، يوفر النظام للمستخدم إمكانية الوصول المناسبة. على سبيل المثال، لنفترض أن لدينا شخصين يعملان في مقهى، لوسيا وراهول. لوسيا هي مديرة المقهى بينما راهول هو باريستا. يستخدم المقهى نظام نقاط البيع (POS) حيث يمكن للنادلين وخبراء صناعة القهوة تقديم الطلبات للتحضير. في هذا المثال، ستستخدم نقطة البيع بعض العمليات للتحقق من هوية Lucia أو Rahul قبل السماح لهما بالوصول إلى النظام. على سبيل المثال، قد يطلب منهم اسم مستخدم وكلمة مرور، أو قد يحتاجون إلى مسح إبهامهم ضوئيًا على قارئ بصمات الأصابع. نظرًا لأن المقهى يحتاج إلى تأمين الوصول إلى نقطة البيع الخاصة به، يحتاج الموظفون الذين يستخدمون النظام إلى التحقق من هويتهم عبر عملية المصادقة.

أنواع المصادقة الشائعة

يمكن للأنظمة استخدام عدة آليات لمصادقة المستخدم. عادةً، للتحقق من هويتك، تستخدم عمليات المصادقة ما يلي: - شيء تعرفه - شيء تملكه - أو شيء أنت عليه

تعد كلمات المرور وأسئلة الأمان من عوامل المصادقة التي تندرج ضمن فئة "شيء تعرفه". وبما أنك وحدك من يعرف كلمة المرور الخاصة بك أو الإجابة على مجموعة معينة من أسئلة الأمان، فإن الأنظمة تستخدم هذا الافتراض لتمنحك حق الوصول.

هناك نوع شائع آخر من عوامل المصادقة يستخدم شيئًا لديك. تندرج الأجهزة المادية مثل رموز أمان USB والهواتف المحمولة ضمن هذه الفئة. على سبيل المثال، عند الوصول إلى نظام ما، ويرسل لك رقم التعريف الشخصي لمرة واحدة (OTP) عبر الرسائل القصيرة أو أحد التطبيقات، يمكنه التحقق من هويتك لأنه جهازك.

يستخدم النوع الأخير من عامل المصادقة شيئًا أنت عليه. تندرج آليات المصادقة البيومترية ضمن هذه الفئة. وبما أن الخصائص الفيزيائية الفردية مثل بصمات الأصابع فريدة من نوعها، فإن التحقق من الأفراد باستخدام هذه العوامل يعد آلية مصادقة آمنة.

**Authorization**

التفويض هو عملية الأمان التي تحدد مستوى وصول المستخدم أو الخدمة. في مجال التكنولوجيا، نستخدم التفويض لمنح المستخدمين أو الخدمات إذنًا للوصول إلى بعض البيانات أو تنفيذ إجراء معين. إذا قمنا بإعادة النظر في مثال المقهى الخاص بنا، فإن راهول ولوسيا لهما أدوار مختلفة في المقهى. نظرًا لأن راهول يعمل باريستا، فلا يجوز له سوى تقديم الطلبات وعرضها. من ناحية أخرى، قد تتمكن لوسيا، بصفتها مديرة، من الوصول إلى إجمالي المبيعات اليومية. وبما أن راهول ولوسيا لهما وظائف مختلفة في المقهى، فإن النظام سيستخدم هويتهما التي تم التحقق منها لتزويد كل مستخدم بأذونات فردية. ومن المهم ملاحظة الفرق هنا بين المصادقة والترخيص. تتحقق المصادقة من المستخدم (Lucia) قبل السماح له بالوصول، ويحدد التفويض ما يمكنه فعله بمجرد أن يمنحه النظام حق الوصول (عرض معلومات المبيعات).

أنواع التفويض الشائعة

توجد أنظمة الترخيص بأشكال عديدة في بيئة تقنية نموذجية. على سبيل المثال، تحدد قوائم التحكم في الوصول (ACLs) المستخدمين أو الخدمات التي يمكنها الوصول إلى بيئة رقمية معينة. إنهم ينجزون التحكم في الوصول هذا من خلال فرض قواعد السماح أو الرفض بناءً على مستوى ترخيص المستخدم. على سبيل المثال، في أي نظام، يوجد عادةً مستخدمون عامون ومستخدمون متميزون أو إداريون. إذا أراد مستخدم قياسي إجراء تغييرات تؤثر على أمانه، فقد ترفض قائمة التحكم بالوصول (ACL) الوصول. ومن ناحية أخرى، يتمتع المسؤولون بالتفويض لإجراء تغييرات أمنية، وبالتالي فإن قائمة التحكم بالوصول (ACL) ستسمح لهم بالقيام بذلك.

نوع آخر شائع من الترخيص هو الوصول إلى البيانات. في أي بيئة مؤسسة، يكون لديك عادةً بيانات ذات مستويات مختلفة من الحساسية. على سبيل المثال، قد يكون لديك بيانات عامة تجدها على موقع الشركة على الويب، وبيانات داخلية لا يمكن الوصول إليها إلا للموظفين، وبيانات سرية لا يمكن الوصول إليها إلا لعدد قليل من الأفراد. في هذا المثال، يحدد الترخيص المستخدمين الذين يمكنهم الوصول إلى أنواع المعلومات المختلفة.

الفرق بين المصادقة والترخيص

كما ذكرنا سابقًا، قد يبدو المصادقة والترخيص متشابهين، لكن يلعب كل منهما دورًا مختلفًا في تأمين الأنظمة والبيانات. لسوء الحظ، غالبًا ما يستخدم الأشخاص كلا المصطلحين بالتبادل حيث يشير كلاهما إلى الوصول إلى النظام. ومع ذلك، فهي عمليات متميزة. ببساطة، يتحقق أحدهما من هوية المستخدم أو الخدمة قبل منحهما حق الوصول، بينما يحدد الآخر ما يمكنه فعله بمجرد حصوله على حق الوصول.

أفضل طريقة لتوضيح الاختلافات بين المصطلحين هي بمثال بسيط. لنفترض أنك قررت الذهاب لزيارة منزل أحد الأصدقاء. عند وصولك، طرقت الباب، فيفتحه صديقك. تتعرف عليك (المصادقة) وتحييك. بما أن صديقتك قد قامت بالمصادقة عليك، فهي الآن مرتاحة للسماح لك بالدخول إلى منزلها. ومع ذلك، بناءً على علاقتك، هناك أشياء معينة يمكنك القيام بها وأشياء أخرى لا يمكنك القيام بها (التفويض). على سبيل المثال، يمكنك الدخول إلى منطقة المطبخ، لكن لا يمكنك الدخول إلى مكتبها الخاص. بمعنى آخر، لديك تصريح بدخول المطبخ، لكن الوصول إلى مكتبها الخاص محظور.

ما هي أوجه التشابه بين التفويض والمصادقة؟

تتشابه المصادقة والتفويض من حيث أنهما جزءان من العملية الأساسية التي توفر الوصول. وبالتالي، غالبًا ما يتم الخلط بين المصطلحين في مجال أمن المعلومات لأنهما يشتركان في نفس الاختصار "auth". تتشابه المصادقة والترخيص أيضًا في الطريقة التي يستفيد بها كل منهما من الهوية. على سبيل المثال، يقوم أحدهما بالتحقق من الهوية قبل منح الوصول، بينما يستخدم الآخر هذه الهوية التي تم التحقق منها للتحكم في الوصول.

المصادقة والترخيص في الحوسبة السحابية

يعد الأمان عنصرًا حيويًا في أي حل للحوسبة السحابية. وبما أن هذه الخدمات توفر نموذج وصول مشترك حيث يتم تشغيل كل شيء على نفس النظام الأساسي، فإنها تحتاج إلى فصل أنظمة العملاء وبياناتهم وحمايتها. يستخدم موفرو الخدمات السحابية المصادقة والترخيص لتحقيق هذه الأهداف الأمنية. في الواقع، لم تتمكن منصات الحوسبة السحابية من توفير اقتصاديات الحجم عبر نموذج الموارد المشتركة الخاص بها دون المصادقة والترخيص.

على سبيل المثال، عندما يحاول مستخدم الوصول إلى خدمة سحابية معينة، سيطالبه النظام ببعض أشكال المصادقة. قد يطلب منهم هذا التحدي إدخال اسم مستخدم وكلمة مرور أو استخدام عامل آخر للتحقق من الهوية، مثل قبول إشعار على أحد التطبيقات. بمجرد مصادقة المستخدم بنجاح، ستستخدم المنصة السحابية بعد ذلك التفويض للتأكد من أنه لا يمكن للمستخدم الوصول إلا إلى أنظمته وبياناته. بدون المصادقة والترخيص، لن يكون من الممكن فصل بيئات العملاء على نفس النظام الأساسي.

أيهما يأتي أولاً، المصادقة أم التفويض؟

تعتمد المصادقة والترخيص على الهوية. نظرًا لأنه لا يمكنك ترخيص مستخدم أو خدمة قبل التعرف عليهم، فإن المصادقة تأتي دائمًا قبل الترخيص. مرة أخرى، يمكننا الرجوع إلى مثال المقهى الخاص بنا لتوضيح هذه النقطة.

كما ذكرنا سابقًا، يمكن لصانعي القهوة إنشاء الطلبات وعرضها فقط، بينما يمكن للمديرين أيضًا الوصول إلى بيانات المبيعات اليومية. إذا لم يتمكن نظام نقطة البيع من تحديد المستخدم الذي يصل إلى النظام، فلن يتمكن من توفير المستوى الصحيح من الوصول. توفر المصادقة تفويض الهوية الذي تم التحقق منه والذي يحتاج إلى التحكم في الوصول. عندما يقوم راهول أو لوسيا بتسجيل الدخول إلى النظام، يعرف التطبيق من قام بتسجيل الدخول والدور الذي يجب أن يحدده لهويتهما.

التحكم في الوصول مقابل المصادقة؟

غالبًا ما يستخدم الأشخاص مصطلحي التحكم في الوصول والترخيص بالتبادل. على الرغم من أن العديد من سياسات الترخيص تشكل جزءًا من التحكم في الوصول، إلا أن التحكم في الوصول يعد أحد مكونات الترخيص. يستخدم التحكم في الوصول عملية التفويض إما لمنح أو رفض الوصول إلى الأنظمة أو البيانات. بمعنى آخر، يحدد الترخيص السياسات المتعلقة بما يمكن للمستخدم أو الخدمة الوصول إليه. التحكم بالوصول يفرض هذه السياسات.

إذا قارنا المصادقة والتحكم في الوصول، فإن المقارنة بين المصادقة والتفويض لا تزال سارية. تتحقق المصادقة من هوية المستخدم، ويستخدم التحكم في الوصول هذه الهوية لمنح الوصول أو رفضه.