
## التحكم في الوصول

يمكن النظر إلى التحكم في الوصول كعنصر مركزي في أمن المعلومات ، تحدد التوصية (ITU-T/X.800) التحكم في الوصول: **"منع الاستخدام غير المصرح به لموارد النظام ، بما في ذلك منع استخدام الموارد بطريقة غير مصرح بها"**

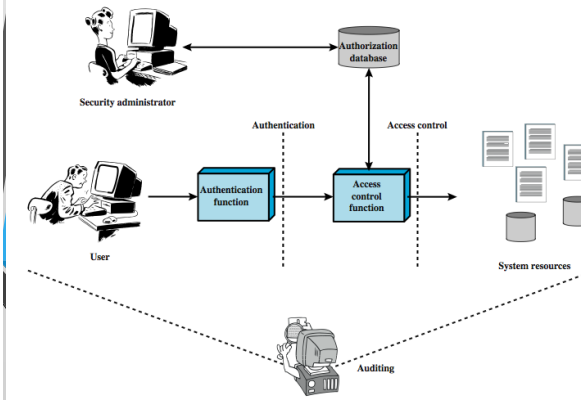
التحكم في الوصول هو تقييد الوصول إلى موارد نظام المعلومات للمصرح لهم فقط من المستخدمين والبرامج والعمليات والنظم. ونحن نتعامل يومياً مع أنظمة التحكم في الوصول، ففي أمن الحواسيب يتمثل التحكم في الوصول من خلال استخدام نماذج او قوائم التحكم في الوصول. ونماذج التحكم في الوصول توضح مدى توافر الموارد في النظام. والنماذج المفيدة في التحكم في الوصول تكون قادرة على تمثيل الحماية المطلوبة للمعلومات والموارد من أي نوع وعلى مستويات متفاوتة من التفاصيل. وفي الوقت نفسه فإن تنفيذ النماذج ينبغي ألا يضع حملا مفرطاً على القدرات الحاسوبية لنظام التشغيل.

**الأهداف :-**

- منع المستخدمين غير المصرح لهم من الوصول إلى الموارد
- منع المستخدمين الشرعيين من الوصول إلى الموارد بطريقة غير مصرح بها
- وتمكين المستخدمين الشرعيين من الوصول إلى الموارد بطريقة مصرح بها
- الأخذ في الاعتبار المجموعات و المستخدمين القادرين على المصادقة على نظام ثم يتم تعيين حقوق الوصول إلى موارد معينة على النظام.

## مبادئ التحكم في الوصول

نتعامل هنا مع مفهوم أضيق وأكثر تحديدًا للتحكم في الوصول، والذي ينفذ سياسة أمنية تحدد من أو ما الذي يمكنه الوصول إليه من موارد نظام محدد، ونوع الوصول المسموح به في كل حالة. يوضح الشكل المفهوم الأوسع للتحكم في الوصول. فبالإضافة إلى التحكم في الوصول ، يشمل هذا المفهوم الأوسع الكيانات والوظائف التالية:




**المصادقة**: التحقق من هوية المستخدم والمطالب بها من قبل النظام أو لصالحه.
**التفويض**: منح حق أو إذن لكيان النظام للوصول إلى موارد النظام. تحدد هذه الوظيفة من يمكن الوثوق به لغرض معين.
**التدقيق**: مراجعة وفحص مستقلين لسجلات وأنشطة النظام من أجل اختبار مدى كفاية ضوابط النظام ، ولضمان الامتثال للسياسة المعمول بها وإجراءات التشغيل ، واكتشاف الانتهاكات الأمنية ، والتوصية بأي تغييرات مشار إليها في الضوابط والسياسات و الإجراءات.

## مبادئ التحكم في الوصول

تتوسط آلية التحكم في الوصول بين المستخدم (أو عملية يتم تنفيذها نيابة عن المستخدم) وموارد النظام ، مثل الملفات وقاعدة البيانات. يجب أن يقوم النظام أولاً بالمصادقة على المستخدم الذى يسعى للوصول. بعد ذلك ، تحدد وظيفة التحكم في الوصول ما إذا كان الوصول المطلوب المحدد من قبل هذا المستخدم مسموحًا به ام لا.

يحتفظ مسؤول الأمان بقاعدة بيانات للتفويضات التي تحدد نوع الوصول إلى الموارد المسموح بها لهذا المستخدم. تستشير وظيفة التحكم في الوصول قاعدة البيانات لتحديد ما إذا كان سيتم منح الوصول أم لا، كما تراقب وظيفة التدقيق وصول المستخدم إلى موارد النظام و وتحتفظ أيضا بسجلات لذلك.

تحتوي جميع أنظمة التشغيل على عنصر تحكم في الوصول بدائي (على الأقل)، وفي بعض الحالات قوي جدًا. تتضمن أيضًا تطبيقات أو أدوات مساعدة معينة ، مثل نظام إدارة قاعدة البيانات ، وفرض وظائف التحكم في الوصول.

## سياسات التحكم في الوصول

- **التحكم في الوصول التقديري:** (Discretionary access control (**DAC**))

استنادًا إلى هوية مقدم الطلب وقواعد الوصول، ويتحكم في الوصول استنادًا إلى هوية مقدم الطلب وعلى قواعد الوصول (التفويضات) التي توضح ما هو مسموح (أو غير مسموح) لمقدمي الطلبات القيام به. تسمى هذه السياسة تقديرية لأن الكيان قد يكون لديه حقوق وصول تسمح له - بمحض إرادته - بتمكين كيان آخر من الوصول إلى بعض الموارد.

- **التحكم في الوصول الإلزامي:** (Mandatory access control (**MAC**))

استنادًا إلى مقارنة وسم الأمان مع التصاريح الأمنية (إلزامي: لا يمكن لمن لديه حق الوصول إلى مورد ما أن يمرره إلى الآخرين) . يتحكم في الوصول استنادًا إلى مقارنة وسم الأمان (التي تشير إلى مدى حساسية موارد النظام أو أهميتها) مع التصاريح الأمنية (التي تشير إلى أن كيانات النظام مؤهلة للوصول إلى موارد معينة). يُطلق على هذه السياسة اسم إلزامي لأن الكيان الذي لديه تصريح للوصول إلى مورد لا يجوز له ، بمحض إرادته ، تمكين كيان آخر من الوصول إلى هذا المورد.

- **التحكم في الوصول المعتمد على الدور (المنصب):** (Role-based access control (**RBAC**))

استنادًا إلى أدوار المستخدم . يتحكم في الوصول استنادًا إلى الأدوار التي يمتلكها المستخدمون داخل النظام وعلى القواعد التي تنص على الوصول المسموح به للمستخدمين في أدوار معينة.

- **التحكم في الوصول المعتمد على السمات:** ( Attribute-based access control(**ABAC**))

استنادًا إلى سمات المستخدم والموارد والبيئة الحالية. يتحكم في الوصول بناءً على سمات المستخدم والمورد الذي سيتم الوصول إليه والظروف البيئية الحالية.

## متطلبات التحكم في الوصول

- **مدخلات موثوقة**: آلية للمصادقة - تفترض أن المستخدم تم التحقق منه؛ وبالتالي، هناك حاجة إلى آلية المصادقة كواجهة أمامية لنظام التحكم في الوصول. يجب أن تكون المدخلات الأخرى لنظام التحكم في الوصول موثوقة أيضًا.
- **المواصفات الدقيقة والصعبة**: تنظيم الوصول على مستويات مختلفة بحيث تسمح المواصفات الدقيقة بالوصول المنظم على مستوى الحقول / السجلات الفردية في الملفات (أوسمة أو قاعدة بيانات كاملة) ؛ ووصول منفرد من قبل مستخدم بدلاً من وصول متسلسل. يجب أن يكون مسؤولو النظام أيضًا قادرين على اختيار مواصفات صعبة لبعض الفئات للوصول إلى الموارد.
- **الامتياز الأقل**: الحد الأدنى من الإذن للقيام بالعمل ، بحيث يتم منح كل كيان في نظام الحد الأدنى من موارد النظام والتراخيص اللازمة للقيام بعمله. يميل هذا المبدأ إلى الحد من الضرر الذي يمكن أن ينجم عن حادث أو خطأ أو عمل غير مصرح به.

## متطلبات التحكم في الوصول

- **فصل المهام**: يجب تقسيم الخطوات في وظيفة ما للنظام بين أفراد مختلفين ، وذلك لمنع فرد واحد من تخريب العملية.
- **السياسات المفتوحة والمغلقة:** تسمح السياسة المغلقة بالوصول فقط للمصرح به على وجه التحديد ؛ تسمح السياسة المفتوحة لجميع عمليات الوصول باستثناء تلك المحظورة صراحة.
- **السياسات وحل التعارضات** : قد تطبق سياسات متعددة على فئة معينة من الموارد ، وهذا قد يحتاج إلى إجراءات خاصة لحل التعارض بين هذه السياسات اذا تداخلت.
- **السياسات الإدارية**: تحديد من يمكنه إضافة قواعد التفويض أو حذفها أو تعديلها ، ويحتاج إلى التحكم في الوصول وآليات التحكم الأخرى لفرض هذه السياسات الإدارية.

## عناصر التحكم في الوصول

- **المستخدم** (Subject): هو الكيان القادر على الوصول إلى المكونات، وعادة ما يكون عملية ما .
- يحصل أي مستخدم أو تطبيق فعليًا على حق الوصول إلى مكون عن طريق عملية تمثله. عادة ما يكون المستخدم مسؤولاً عن الإجراءات التي بدأها ، ويمكن استخدام خيارات التدقيق لربط المستخدم واجراءات الامن التي ذات العلاقة التي تم تنفيذها على مكون ما.
- تحدد أنظمة التحكم في الوصول الأساسية (عادة) ثلاث فئات من المستخدمين:
  - **المالك**: قد يكون هو منشئ المورد، مثل ملف. بالنسبة لموارد النظام، قد تكون الملكية إلى مسؤول النظام. بالنسبة لموارد مشروع ، قد يتم تكون الملكية إلى مسؤول المشروع أو المدير.
  - **المجموعة**: بالإضافة إلى الامتيازات المعينة للمالك ، يمكن أيضًا منح مجموعة محددة من المستخدمين حقوق الوصول ، بحيث تكون العضوية في المجموعة كافية لممارسة حقوق الوصول هذه.
  - **العام**: يتم منح أقل قدر من الوصول للمستخدمين القادرين على الوصول إلى النظام ولكن لم يتم تضمينهم في فئات المالك والمجموعة لهذا المورد.
- **المكون** (Object) : هو أي مورد يتم التحكم في الوصول إليه. بشكل عام ، المكون هو كيان يستخدم لاحتواء و/ أو تلقي المعلومات.
- على سبيل المثال السجلات والقوالب والصفحات والمقاطع والملفات وأجزاء من الملفات والأدلة وتفرعات الادلة وصناديق البريد والرسائل والبرامج.
- يعتمد عدد وأنواع المكونات التي يجب حمايتها بواسطة نظام التحكم في الوصول على البيئة التي يتم فيها التحكم في الوصول.
- **حق الوصول** (Access Right) : يصف حق الوصول الطريقة التي يمكن للمستخدم من خلالها الوصول إلى المكون، ويمكن أن تشمل حقوق الوصول ما يلي: قراءة ، كتابة ، تنفيذ ، حذف ، إنشاء ، بحث.

## التحكم في الوصول التقديري (DAC)

التحكم في الوصول التقديري هو قائمة من الأذونات تتبع مكونات محددة. وتستخدمُ قوائم التحكم في الوصول جَملًا بسيطة لتحديد المستخدمين (subjects) والمكونات (objects) والعمليات المسموح بها. ويقوم نظام التشغيل بالتحقق من طلبات الموارد الواردة بهدف معرفة مدخلات قائمة التحكم في الوصول التي قد تمنع الوصول إلى الموارد.

وُتستخدم قوائم التحكم في الوصول التقديرى عادة للدفاع عن نوعن من الموارد: الملفات واتصالات الشبكات. وتقوم (قوائم التحكم في الوصول لحماية الملفات) بتحديد حقوق المستخدمين، سواء كانوا أفراداً أم جماعات، وذلك للوصول إلى الملفات والملفات التنفيذية. وتقوم (قوائم التحكم في الوصول لحماية اتصالات الشبكات) بتحديد القواعد لمعرفة أرقام المنافذ والعناوين الشبكية التي يمكن الوصول إليها. وتعد (قوائم التحكم في الوصول إلى حماية اتصالات الشبكات) أحد الطرق الشائعة في تطبيق الجُدر النارية. ومعظم أنظمة التشغيل الحديثة تأتي بقوائم تحكم وصول افتراضيةُ والتي توفر مستويات معقولة من الأمن للمستخدم العادي. وتعد قوائم التحكم في الوصول من أبسط الضوابط في التطبيق، كما تعتمد فاعلية العديد من الضوابط الأمنية الأخرى على قوائم التحكم في الوصول. على سبيل المثال، تساعد قوائم التحكم في الوصول إلى المحافظة على تكامل وجاهزية كلمات المرور عن طريق منع المهاجمين من الكتابة فوق كلمات المرور.

## التحكم في الوصول التقديري

تتمثل الطريقة العامة للتحكم في الوصول كما ينفذها نظام التشغيل أو نظام إدارة قاعدة البيانات في **مصفوفة الوصول**.

- غالبًا ما تكون على شكل مصفوفة وصول ، احد ابعاد المصفوفة توجد بها المستخدمين (الصفوف) ، وتوجد المكونات في البعد الآخر (الأعمدة). تحدد كل خلية حقوق وصول المستخدم المحددة لهذا المكون. مصفوفة الوصول يمكن تقسيمها/تحليلها عن طريق أي صف أو عمود
- **البعد الأول** للمصفوفة يتكون من فئة محددة من المستخدمين التي قد تحاول الوصول إلى البيانات. عادةً ما تتكون هذه القائمة من مستخدمين فرادى أو مجموعات ، مع إمكانية التحكم في الوصول للأجهزة الطرفية أو الأجهزة المضيفة أو التطبيقات بدلاً من المستخدمين أو بالإضافة إليهم.

## التحكم في الوصول التقديري (DAC)

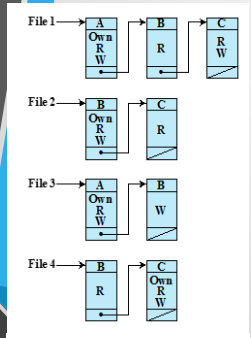
- **البعد الثاني** يتكون من المكونات التي يمكن الوصول إليها. في أعلى مستوى من التفاصيل ، قد تكون المكونات عبارة حقول بيانات فردية. وقد تكون عبارة عن مجموعات مجمعة ، مثل السجلات أو الملفات أو حتى قاعدة البيانات بأكملها ، أو كائنات في المصفوفة. تشير كل خلية في المصفوفة إلى حقوق الوصول لهذا المستخدم على هذا المكون. من الناحية العملية ، مصفوفة الوصول يمكن انجازها عن طريق تقسيمها بإحدى طريقتين ، كما سيتم عرضه تاليا.

| | | OBJECTS | | | |
|---|---|---|---|---|---|
| | | File 1 | File 2 | File 3 | File 4 |
| SUBJECTS | User A | Own Read Write | | Own Read Write | |
| | User B | Read | Own Read Write | Write | Read |
| | User C | Read Write | Read | | Own Read Write |

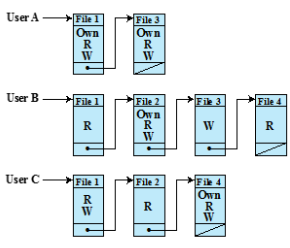
(a) Access matrix

## بنية بيانات التحكم في الوصول

- قوائم التحكم في وصول المستخدمين (موزعة حسب العمود)
- اذونات الاستخدام (موزعة حسب الصف)
- لاحظ أيضًا التمثيل البديل لجدول الاذونات




قوائم التحكم في الوصول للملفات في مصفوفة الوصول السابقة




قوائم الاذونات للملفات في مصفوفة الوصول السابقة

**التمثيل البديل لجدول الاذونات**

| Subject | Access Mode | Object |
|---|---|---|
| A | Own | File 1 |
| A | Read | File 1 |
| A | Write | File 1 |
| A | Own | File 3 |
| A | Read | File 3 |
| A | Write | File 3 |
| B | Read | File 1 |
| B | Own | File 2 |
| B | Read | File 2 |
| B | Write | File 2 |
| B | Write | File 3 |
| B | Read | File 4 |
| C | Read | File 1 |
| C | Write | File 1 |
| C | Read | File 2 |
| C | Own | File 4 |
| C | Read | File 4 |
| C | Write | File 4 |

## التحكم في الوصول التقديري : (مثال)

وتبدأ قوائم التحكم في الوصول من الفرق الأساسي بين الأشخاص والمكونات. فالأشخاص يحاولون تنفيذ العمليات على المكونات، ويتم السماح بتنفيذ العمليات إذا كان ذلك مسموحاً من قبل قوائم التحكم في الوصول. ويمكن تمثيل قوائم التحكم في الوصول باعتبارها (مصفوفة وصول) تقوم بتحديد الأذونات لكل شخص وعلى كل مكون. ويوضح الشكل مثالاً على ذلك.

**مثال على مصفوفة وصول**

| | | المكونات | | |
|---|---|---|---|---|
| | | قاعدة البيانات | الملف-1 | الملف-2 |
| المستخدمين | مستخدم-1 | حظر | مالك قراءة كتابة | قراءة |
| | مستخدم-2 | حظر | قراءة | قراءة |
| | مستخدم-3 | مسموح | تنفيذ | مالك قراءة كتابة تنفيذ |

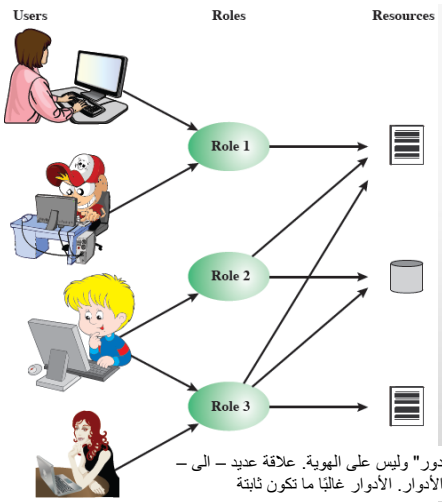
وتوضح كل خلية في الشكل أذونات الوصول للشخص المقابل والمستخدم للمكون المقابل. المستخدم-1 هو مالك الملف رقم (1) ، كما أن لديه أذونات قراءة وكتابة على الملف. وأن المستخدم-1مالك الملف يمكنه تعيين أذونات على الملف لأي شخص. وفي هذه الحالة تم إعطاء المستخدم-2 إذن قراءة الملف، كما تم إعطاء المستخدم-3 إذن التنفيذ على الملف. وهكذا فإن كل خلية تمثل قائمة تحكم في الوصول لكل مستخدم للمكون المقابل.

القيود: تُعد قوائم التحكم في الوصول آلية بسيطة جداً لكنها فعالة لمراقبة الوصول. ومع ذلك فهي لا تخلو من بعض القيود الهامة. فإذا كان يجب تعديل الأذونات لمستخدم معين، فإنه يجب تعديل الأذونات على جميع المكونات التي تمكن هذا المستخدم من الوصول إليها. وأيضاً فإنه ليس من الممكن تعيين أذونات على أساس مسؤوليات المستخدم. فإذا تم تغيير دور المستخدم فإن منح أذونات الوصول المناسبة للدور الجديد لهذا المستخدم يتطلب تعديل الأذونات لكل مستخدم على حدة، وذلك على جميع المكونات ذات العلاقة.

## التحكم في الوصول المعتمد على الدور (المنصب) - (RBAC)

تحدد أنظمة التحكم في الوصول التقديري التقليدية حقوق الوصول للمستخدمين فرادى ومجموعات المستخدمين. في المقابل ، يعتمد نظام التحكم في الوصول المعتمد على الدور على الأدوار المفترضة للمستخدمين على النظام بدلاً من هوية المستخدم.

عادة ، تحدد نماذج نظام التحكم في الوصول المعتمد على الدور المنصب كمهمة وظيفية داخل المؤسسة، حيث أن التحكم في الوصول المعتمد على الدور يعين الأذونات للمستخدمين بناءً على الدور بدلاً من تعيينها بناء على المستخدم الفردي حيث يتم إنشاء الأدوار لمهام العمل، ويتم تعيين أدوار مختلفة المستخدمين ، إما بشكل ثابت أو ديناميكي ، وفقًا لمسؤولياتهم. ومن خلال تحديد أذونات الوصول للأدوار، هناك فرق بين ضوابط المستخدم، وضوابط الوصول. فالمستخدمون يتطورون تدريجياً في المؤسسة، أدوارهم او مناصبهم يمكن تعيينها، وأذونات الوصول يتم تحديثها تلقائياً. لذا عند مقارنة التحكم في الوصول المعتمد على الدور بقوائم التحكم في الوصول فإن الأول يقلل من التكاليف ومن الجهد الإداري المطلوب لتنفيذ التحكم في الوصول في المؤسسات الكبيرة.




الوصول على أساس "الدور" وليس على الهوية. علاقة عديد – الى – عديد بين المستخدمين والأدوار. الأدوار غالبًا ما تكون ثابتة

## التحكم في الوصول المعتمد على الدور

قبل منح صلاحيات الوصول لأي من موارد المؤسسة يتوجب على مسؤول الأمن وعلى قيادة المؤسسة تطوير سياسات لتنظيم كيفية منح الوصول. وفي نظام التحكم في الوصول المعتمد على الدور، فإن الأذونات الازمة لتنفيذ مجموعة من العمليات المرتبطة ببعضها يتم اعتبارها دوراً من أدوار النظام. كما يتم ربط أدوار النظام المِعتمد على تلك بمهام وظيفة أو وظائف محددة في المنظمة. ونظام التحكم في الوصول المعتمد على الدور يمنح الأفراد ذوي الأدوار المحددة امتيازات وصول تتناسب مع أدوار النظام المناظرة لها. على سبيل المثال، قد يسمح للشخص الذي يعمل وكيل مشتريات بإدخال أمر شراء جديد، لكن لا يُسمح له بالموافقة على الدفع بحيث تمنح القدرة على الموافقة على الدفع لدور مرتبط بشخص في وظيفة مختلفة مثل المحاسبة. وتعرف الحالة التي يقوم فيها أكثر من شخص بإتمام مهمة كاملة بحالة **فصل المهام**. وتعد حالة فصل المهام سمة مشتركة في أنظمة الأعمال وخاصة عندما يتعلق الأمر بالمعاملات النقدية.

ويهدف نظام التحكم في الوصول المعتمد على الدور إلى جعل السياسات الأمنية تعكس العمليات الفعلية للمنظمة. وكل فرد في المنظمة ينبغي أن يمنح فقط الأدوار الضرورية جداً لإتمام عمله بنجاح، وكل دور يجب أن يحتوي فقط على الأذونات الازمة لأداء المهام المحددة. وبما أن نموذج نظام التحكم في الوصول المعتمد على الدور يرتبط مباشرة بالوظائف الحقيقية لأفراد في المؤسسة، يستطيع مسؤولو أمن المعلومات العمل مباشرة مع مستخدمي النظام والمسؤولين عن العمليات، وذلك بهدف تطوير السياسات التي سيتم تطبيقها. وهذا الأمر مهم لأن مستخدمي النظام هم الخبراء في هذا الموضوع، فالمستخدمون يعرفون أذونات النظام الازمة لوظيفة معينة، كما يعرفون المهام الوظيفية المرتبطة بوظيفة معينة.

## التحكم في الوصول المعتمد على الدور

- **علاقة المستخدمين بالأدوار هي على شكل عديد – الى – عديد** ، كما هو الحال بالنسبة لعلاقة الأدوار بالموارد ، أو مكونات النظام ، كما هو موضح في الشكل السابق.
- **تتغير مجموعة المستخدمين** في بعض البيئات بشكل متكرر ، وقد يتم تحديد دور واحد أو أكثر لمستخدم ما ديناميكيًا.
- في معظم البيئات غالبا ما يكون **تحديد الدور في النظام ثابتا** ، مع عمليات إضافة أو حذف عرضية فقط.
- **يكون لكل دور حقوق وصول محددة إلى مورد واحد أو أكثر**. كذلك ، الموارد وحقوق الوصول الخاصة المرتبطة بدور معين غالبا ما تتغير بشكل غير متكرر.

**مصفوفة المستخدمين-الادوار**

| | $R_1$ | $R_2$ | ... | $R_n$ |
|---|---|---|---|---|
| $U_1$ | X | | | |
| $U_2$ | X | | | |
| $U_3$ | | X | | X |
| $U_4$ | | | | X |
| $U_5$ | | | | X |
| $U_6$ | | | | X |
| ... | | | | |
| $U_m$ | X | | | |

يمكننا استخدام تمثيل مصفوفة الوصول لتوضيح العناصر الرئيسية لنظام (RBAC) بعبارات بسيطة ، كما هو موضح في الشكل. المصفوفة العليا تربط المستخدمين الفرادى بالمناصب. عادةً ما يكون عدد المستخدمين أكثر من عدد المناصب. كل خلية في المصفوفة تكون إما فارغة أو محددة ، وتشير الأخيرة إلى أن هذا المستخدم قد تم تعيينه لهذا الدور.

**مصفوفة الأدوار-المكونات**

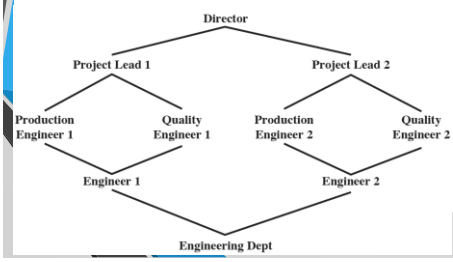
| | OBJECTS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ROLES | $R_1$ | $R_2$ | $R_n$ | $F_1$ | $F_1$ | $P_1$ | $P_2$ | $D_1$ | $D_2$ |
| $R_1$ | control | owner | owner control | read * | read owner | wakeup | wakeup | seek | owner |
| $R_2$ | | control | | write * | execute | | | owner | seek * |
| ... | | | | | | | | | |
| $R_n$ | | | control | | write | stop | | | |

## التحكم في الوصول المعتمد على الدور

- قد يتم تعيين مناصب متعددة لمستخدم واحد (أكثر من علامة واحدة في صف واحد) وأنه قد يتم تعيين عدة مستخدمين لمنصب واحد (أكثر من علامة واحدة في عمود). المصفوفة السفلية لها نفس بنية مصفوفة التحكم في الوصول التقديري مع تمثيل الأدوار كمستخدمين . عادة ، هناك عدد قليل من الأدوار والعديد من المكونات أو الموارد. في هذه المصفوفة ، مدخلات الخلية هي حقوق الوصول المحددة التي تتمتع بها الأدوار. لاحظ أنه يمكن معاملة الدور كا مكون ، مما يسمح بتعريف التدرجات الهرمية للدور.
- التحكم في الوصول المعتمد على الدور يفسح المجال للتنفيذ الفعال لمبدأ الامتياز الأقل، حيث يحتوي كل دور على الحد الأدنى من مجموعة حقوق الوصول اللازمة لهذا الدور. يتم تعيين مستخدم لدور يمكّنه من أداء ما هو مطلوب فقط حسب الدور. العديد من المستخدمين المعينين لنفس الدور يتمتعون بنفس الحد الأدنى من مجموعة حقوق الوصول.

## التحكم في الوصول المعتمد على الدور :- خصائص

- **المكونات :**
  - المستخدم: الشخص الذي يمكنه الوصول إلى نظام الحاسب وله معرف مرتبط به.
  - الدور: مهمة وظيفية محددة داخل المؤسسة تتحكم في نظام الحاسب. عادة ما يرتبط كل دور بوصف للسلطة والمسؤولية الممنوحة لهذا الدور والمستخدم الذى يتولى هذا الدور.
  - الأذن: الموافقة على وضع معين للوصول إلى مكون واحد أو أكثر. (حق الوصول، الامتياز، الترخيص).
  - الجلسة: ربط ما بين المستخدم ومجموعة فرعية نشطة من مجموعة الأدوار التي تم تعيينها إليه.
- **التسلسل الهرمي للأدوار**: توفر التسلسلات الهرمية للأدوار وسيلة لعكس الهيكل الهرمي للأدوار في المؤسسة. عادةً ما تتمتع الوظائف ذات المسؤولية الأكبر بسلطة أكبر للوصول إلى الموارد. قد يكون لوظيفة عمل ثانوية مجموعة محدودة من حقوق الوصول من قبل وظيفة عمل العليا. تستفيد التسلسلات الهرمية للأدوار من مفهوم الوراثة لتمكين دور واحد من تضمين حقوق الوصول المرتبطة بدور ثانوي ضمنيًا، وتكون الأدوار الثانوية أقل عادة.




يشير الخط الفاصل بين دورين إلى أن الدور العلوي يتضمن جميع حقوق الوصول الخاصة بالدور الأدنى ، بالإضافة إلى حقوق الوصول الأخرى غير المتاحة للدور الأدنى. يمكن لدور واحد أن يرث حقوق الوصول من عدة أدوار ثانوية. يمكن أن يرث أكثر من دور من نفس الدور الثانوي.

## التحكم في الوصول المعتمد على الدور :- خصائص

**القيود (الشروط) الواجبة في الأدوار :**

توفر القيود وسيلة لتكييف نظام حق الوصول مع خصوصيات السياسات الإدارية والأمنية في المؤسسة. القيد هو علاقة محددة بين الأدوار أو شرط متعلق بالأدوار. يسرد الأنواع التالية من القيود: **الأدوار الحصرية ، والعلاقة الأساسية ، والمتطلبات الأساسية المسبقة** (الاسبقيات).

- **الأدوار الحصرية** هي الأدوار التي تفرض تخصيص دور واحد فقط للمستخدم من مجموعة الادوار. يمكن أن يكون هذا القيد ثابتًا، أو ديناميكيًا، بحيث يمكن ان يخصص للمستخدم دور واحد فقط من مجموع الأدوار في الجلسة الواحدة. القيد الحصري يدعم الفصل بين المسؤوليات والقدرات داخل المؤسسة. ويمكن تعزيز هذا الفصل أو تعزيزه باستخدام تخصيص الأذونات الحصرية للطرفين. مع هذا القيد الإضافي، تتضمن الأدوار الحصرية على الخصائص التالية: **1**. لا يمكن تعيين مستخدم إلا لدور واحد في المجموعة (إما أثناء جلسة أو بشكل ثابت). **2**. يمكن منح أي إذن (حق الوصول) لدور واحد فقط من المجموعة. وبالتالي فإن مجموعة الأدوار الحصرية لها أذونات غير متداخلة. إذا تم تعيين مستخدمين لأدوار مختلفة في المجموعة، فسيكون لدى المستخدمين أذونات غير متداخلة أثناء تولي هذه الأدوار. الغرض من الأدوار الحصرية هو زيادة صعوبة التواطؤ بين الأفراد ذوي المهارات المختلفة أو الوظائف الوظيفية المتباينة لإحباط السياسات الأمنية.
- تشير **العلاقة الأساسية** إلى تحديد الحد الأقصى لعدد الأدوار، بمعنى تعيين الحد الأقصى لعدد المستخدمين الذين يمكن تعيينهم لدور معين. على سبيل المثال ، قد يقتصر دور مدير المشروع أو دور رئيس القسم على مستخدم واحد. يمكن للنظام أيضًا أن يفرض قيودًا على عدد الأدوار التي يتم تعيين المستخدم لها ، أو عدد الأدوار التي يمكن للمستخدم تنشيطها في الجلسة الواحدة. شكل آخر من أشكال القيد هو تعيين الحد الأقصى لعدد الأدوار التي يمكن منحها إذنًا معينًا ؛ قد يكون هذا أسلوبًا مرغوبًا لتخفيف من مخاطر الحصول على إذن حساس أو قوي.
- قد يكون النظام قادرًا على تحديد **المتطلبات الأساسية المسبقة** (الاسبقيات)، والذي يفرض أنه لا يمكن تعيين دور معين لمستخدم إلا إذا كان قد تم فعليا تعيين دور محدد أخر مسبقا. يمكن استخدام الاسبقيات كشرط أساسي لهيكلة تنفيذ مفهوم الامتيازات الأقل. في التسلسل الهرمي ، قد يكون مطلوبًا أن يتم تعيين مستخدم إلى دور كبير (أعلى) فقط إذا كان قد تم تعيينه مسبقا دورًا صغيرًا (أدنى).

## التحكم في الوصول المستند إلى السمات (ABAC)

من التطورات الحديثة نسبيًا في تقنية التحكم في الوصول اسلوب التحكم في الوصول المستند إلى السمات (ABAC) . يمكن في هذا الأسلوب تحديد الصلاحيات التي تعبر عن شروط خصائص كل من المورد والكيان.

على سبيل المثال، خذ في اعتبارك تكوين ما يحتوي فيه كل مورد على سمة تحدد الكيان الذي أنشأ المورد. اذن ، يمكن لقاعدة وصول واحدة تحديد امتياز الملكية لمنشئي كل مورد. تكمن قوة اسلوب (ABAC) في مرونته وقوته التعبيرية. العقبة الرئيسية أمام اعتمادها في الأنظمة الحقيقية هي القلق بشأن التأثير على الأداء عند التقييم المستند على كل من خصائص الموارد والمستخدم في كل وصول. ومع ذلك ، بالنسبة للتطبيقات مثل خدمات الويب المشتركة والحوسبة السحابية ، فإن تكلفة الأداء المتزايدة نتيجة لوجود تكلفة أداء عالية نسبيًا لكل وصول. وبالتالي ، كانت خدمات الويب رائدة في مجال التقنيات المنفذة لأسلوب (ABAC) ، وهناك اهتمام كبير بتطبيق أسلوب (ABAC) على الخدمات السحابية.

هناك ثلاثة عناصر رئيسية في اسلوب (ABAC) : **السمات** التي يتم تحديدها للكيانات في التكوين ؛ **السياسة** التي تحدد سياسات (ABAC)؛ و**البنية** التي تطبق على السياسات التي تفرض التحكم في الوصول.

## أنواع السمات

السمات هي الخصائص التي تحدد جوانب معينة للكيان ، والمكون ، وظروف البيئة ، و/أو العمليات المطلوبة المحددة مسبقًا والمخصصة مسبقًا من قبل المؤسسة. تحتوي السمات على معلومات تشير إلى فئة المعلومات المقدمة كالسمة ، والاسم ، والقيمة , على سبيل المثال ،

( e.g., Class = HospitalRecordsAccess ،Name = PatientInformationAccess ،Value = MFBusinessHoursOnly ).

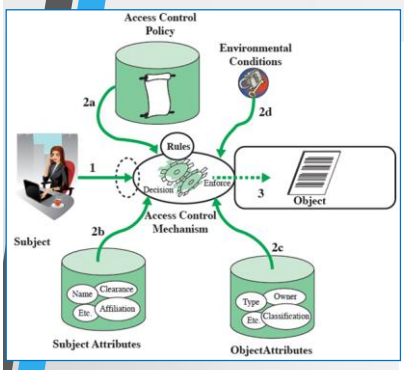
فيما يلي ثلاثة أنواع من السمات في أسلوب (ABAC) :

- **سمات المستخدم** : المستخدم هو كيان نشط (على سبيل المثال ، مستخدم أو تطبيق أو عملية أو جهاز) يتسبب في تدفق المعلومات بين المكونات أو تغيير حالة النظام. كل كيان له سمات مرتبطة به تحدد هوية وخصائص الكيان. قد تتضمن هذه السمات معرف الكيان والاسم والمؤسسة وعنوان المهمة وما إلى ذلك. يمكن أيضًا ان ينظر لدور الكيان كسمة.
- **سمات المكون**: المكون، الذي يشار إليه أيضًا باسم المورد، هو كائن سلبي (في سياق طلب محدد) مرتبط بنظام المعلومات (مثل الأجهزة والملفات والسجلات والجداول والعمليات والبرامج والشبكات والنطاقات) يحتوي على معلومات أو يتلقاها. كما هو الحال مع الكيانات ، تتضمن المكونات سمات يمكن الاستفادة منها لاتخاذ قرارات التحكم في الوصول. قد يحتوي مستند (ميكروسوفت وورد)، مثالا، على سمات مثل العنوان والموضوع والتاريخ والمؤلف. غالبًا ما يمكن استخراج سمات المكون من البيانات الأولية للكائن.
- **سمات البيئة**: وهى تصف البيئة التشغيلية والتقنية وحتى الظرفية أو السياق الذي يحدث فيه الوصول إلى المعلومات. على سبيل المثال ، لا ترتبط السمات ، مثل التاريخ والوقت الحاليين وأنشطة الفيروسات/التسلل الحالية ومستوى أمان الشبكة (على سبيل المثال ، الإنترنت مقابل الإنترانت) بكيان معين أو مورد معين ، ولكنها قد تكون مع ذلك ذات صلة بـتطبيق سياسة التحكم في الوصول.

## البنية المنطقية لنظام (ABAC)

(ABAC) هو أسلوب منطقي للتحكم في الوصول يمكن تمييزه لأنه يتحكم في الوصول إلى المكونات من خلال تقييم القواعد مقابل سمات الموضوعات (الكيان والمكون) والعمليات والبيئة ذات الصلة بالطلب. تعتمد (ABAC) على تقييم سمات الكيان ، وسمات المكون ، والعلاقة الرسمية أو قاعدة التحكم في الوصول التي تحدد العمليات المسموح بها لسمات الكيان-المكون المشتركة في بيئة معينة. تحتوي جميع حلول (ABAC) على هذه القدرات الأساسية لتقييم السمات وفرض القواعد أو العلاقات بين تلك السمات. أنظمة (ABAC) قادرة على فرض مفاهيم (DAC) و (RBAC) و (MAC). يتيح (ABAC) التحكم الدقيق في الوصول، والذي يسمح باستغلال عدد كبير من المدخلات المنفصلة في قرار التحكم في الوصول ، مما يوفر مجموعة كبيرة من التشكيلات الممكنة من تلك المتغيرات لتعكس مجموعة أكبر وأكثر تحديدًا من القواعد أو السياسات أو القيود المحتملة على الوصول. وبالتالي ، يسمح (ABAC) بدمج عدد غير محدود من السمات لتلبية أي قاعدة للتحكم في الوصول. علاوة على ذلك ، يمكن تنفيذ أنظمة (ABAC) لتلبية تشكيلات واسعة من المتطلبات لقوائم التحكم في الوصول الأساسية من خلال نماذج السياسة التعبيرية المتقدمة التي تستفيد بشكل كامل من مرونة (ABAC).

## البنية المنطقية لنظام (ABAC)




يوضح الشكل البيئة المنطقية للمكونات الأساسية لنظام (ABAC). وصول الكيان إلى المكون يتم وفقًا للخطوات التالية:

1. كيان ما يطلب الوصول إلى مكون ما. يتم توجيه هذا الطلب إلى آلية التحكم في الوصول.
2. تخضع آلية التحكم في الوصول لمجموعة من القواعد (2a) التي تم تحديدها من قبل سياسة تحكم في الوصول معدة مسبقا. بناءً على هذه القواعد ، تقوم آلية التحكم في الوصول بتقييم سمات الكيان (2b) والمكون (2c) والظروف البيئية الحالية (2d) لتحديد التفويض.
3. آلية التحكم في الوصول تمنح الكيان الوصول إلى المكون إذا كان مسموحًا بالوصول ويرفض الوصول إذا لم يكن مصرحًا به.

يتضح من البنية المنطقية أن هناك أربعة مصادر مستقلة للمعلومات المستخدمة في قرار التحكم في الوصول. يمكن لمصمم النظام تحديد السمات المهمة للتحكم في الوصول فيما يتعلق بالكيانات والمكونات والظروف البيئية. يمكن لمصمم النظام أو أي سلطة أخرى بعد ذلك تحديد سياسات التحكم في الوصول ، في شكل قواعد لأي مزيج مرغوب من سمات الكيان ، والمكون ، والظروف البيئية. يجب أن يكون واضحًا أن هذا النهج قوي جدًا ومرن. ومع ذلك ، فإن التكلفة ، من حيث تعقيد التصميم والتنفيذ ومن حيث التأثير على الأداء ، من المرجح أن تتجاوز تكلفة نُهج التحكم في الوصول الأخرى، هذه مقايضة يجب أن تقوم بها ادارة النظام.

## Apple

اكتشفت عملاق المعلوماتية ثغرة أمنية خطيرة يوفّر النفاذ إلى الهاتف والجهاز اللوحي ويسمح للقرصان المعلوماتي بالتلاعب به. أي الهواتف والأجهزة اللوحية المعنية بالمشكلة؟ وما العمل لحماية جهازك؟

- أوصت "آبل" أصحاب بعض النماذج من هواتف "آي فون" وأجهزة "آي باد" اللوحية وحواسيب "ماك" بتحديث برنامج التشغيل الذي تشوبه ثغرة أمنية تتيح التحكّم بهذه الأجهزة. وتطال هذه المشكلة النسخة السادسة من هواتف "آي فون" والنسخ التالية وكلّ أجهزة "آي باد برو" والجيل الخامس من "آي باد" والأجيال اللاحقة وكلّ حواسيب "ماك"، وفق ما جاء في الموقع الإلكتروني للشركة التي تتّخذ في كوبرتينو (ولاية كاليفورنيا) مقرّا لها.
- وكشفت "آبل" أن النسخة السابقة من برنامج التشغيل تتضمّن "تطبيقا قد يتيح استخدام رمز تعسفي" يوفّر النفاذ إلى الجهاز ويسمح للقرصان المعلوماتي بالتلاعب به.
- وأشارت "آبل" إلى إنه "من الممكن أن تكون هذه الإمكانية قد استغلّت" من قبل قراصنة معلوماتية، من دون مزيد من التفاصيل. وأردفت أنه من الممكن استغلال هذه الثغرة بواسطة "محتويات انترنت خبيثة".
- ولإصلاح الخلل، حثّت "آبل" المستخدمين على تحميل النسخة 15.6.1 من برنامج التشغيل "آي او اس" لهواتف "آي فون" و"آي باد او اس" 15.6.1 لأجهزة "آي باد" و"ماك او اس مونتيري" 12.5.1 لحواسيب "ماك".
- وأفادت المجموعة الأمريكية بأن باحثين لم تكشف عن هويتهم أبلغوها بوجود الثغرة.
- ويولي عملاق المعلوماتية أهمية قصوى لحماية البيانات الشخصية وللأمن السيبراني. وفي نيسان/أبريل 2021، ألزمت التطبيقات المستخدمة على هواتف "آي فون" بالحصول على إذن المستخدمين إذا ما أرادوا أن تجمع بيانات عنهم بشأن استخدام تطبيقات أخرى وتصفّح الانترنت. وحرم هذا التعديل في نظام "آي او اس" تطبيقات تعوّل كثيرا على الإعلانات، مثل "فيسبوك" و"سنابتشات"، من أدوات قيّمة كانت تدرّ عليها عائدات إعلانية كبيرة.