

# أمن الحاسبات والمعلومات

## الفصل الخامس: نظم التحكم بالوصول

إعداد الدكتور / أسامة حسام الدين

كلية علوم وهندسة الحاسبات يمينع  
جامعة طيبة



# محتوى الفصل الخامس

• نقدم في هذا الفصل طرق التحكم بالوصول

1. المصادقة

2. المنح أو التفويض

3. المتابعة أو الرقابة

# نظم التحكم بالوصول

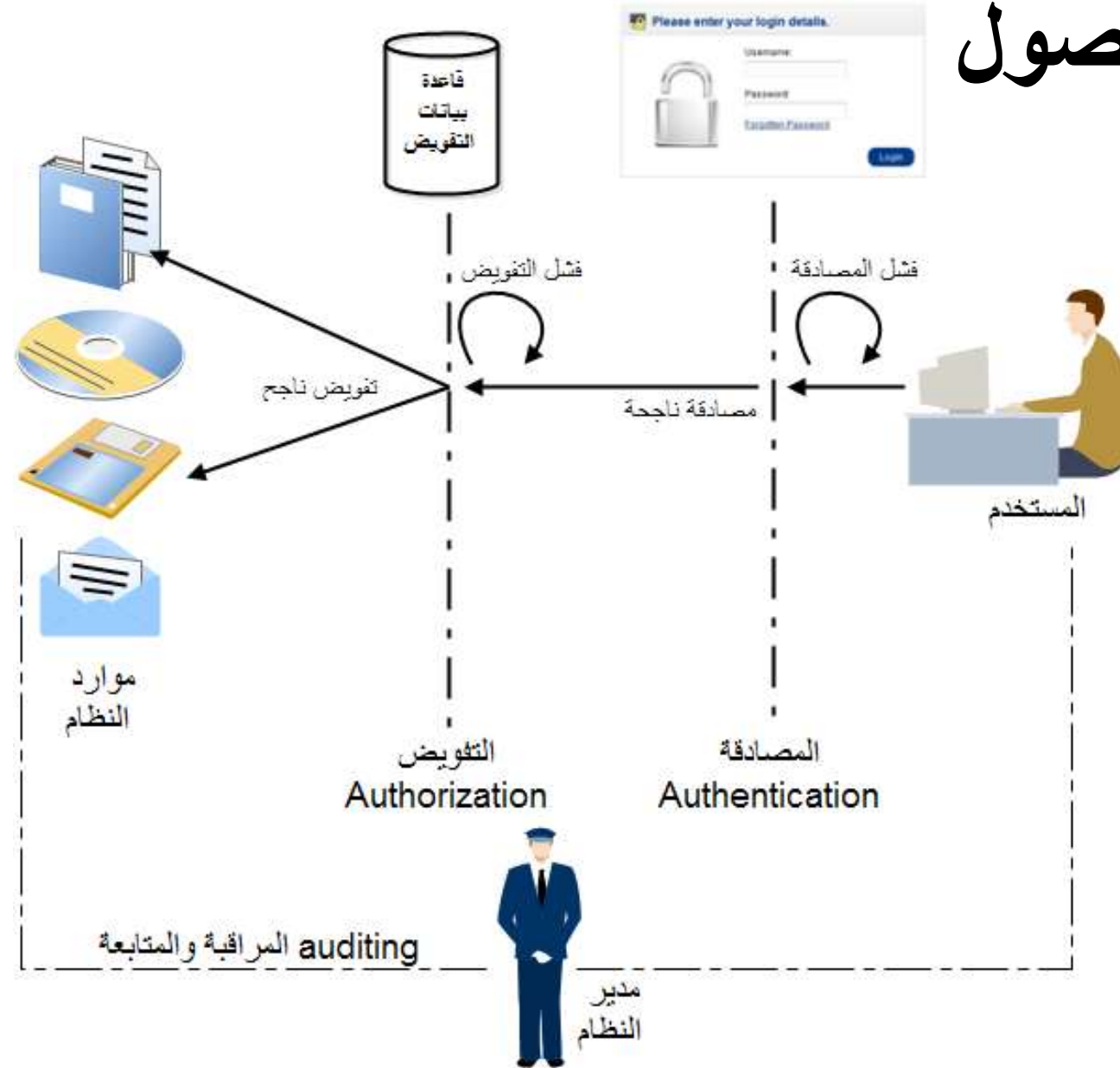
التحكم بالوصول يعني تحجيم الوصول للملفات أو الحاسبات أو شبكات الحاسب أو قواعد البيانات ومنع الوصول إليها من أي شخص أو مورد إلا إذا أعطي الصلاحية لذلك.

تتكون عملية التحكم بالوصول من ثلاث مراحل رئيسية هي:

- المصادقة Authentication
- المنح Authorization
- المتابعة Accounting
- (مبدأ الثلاث ميمات "م م م" وخادم م م م AAA هو خادم خاص يقوم بعمل تلك المراحل الثلاث بطريقة مركزية

# نظم التحكم بالوصول

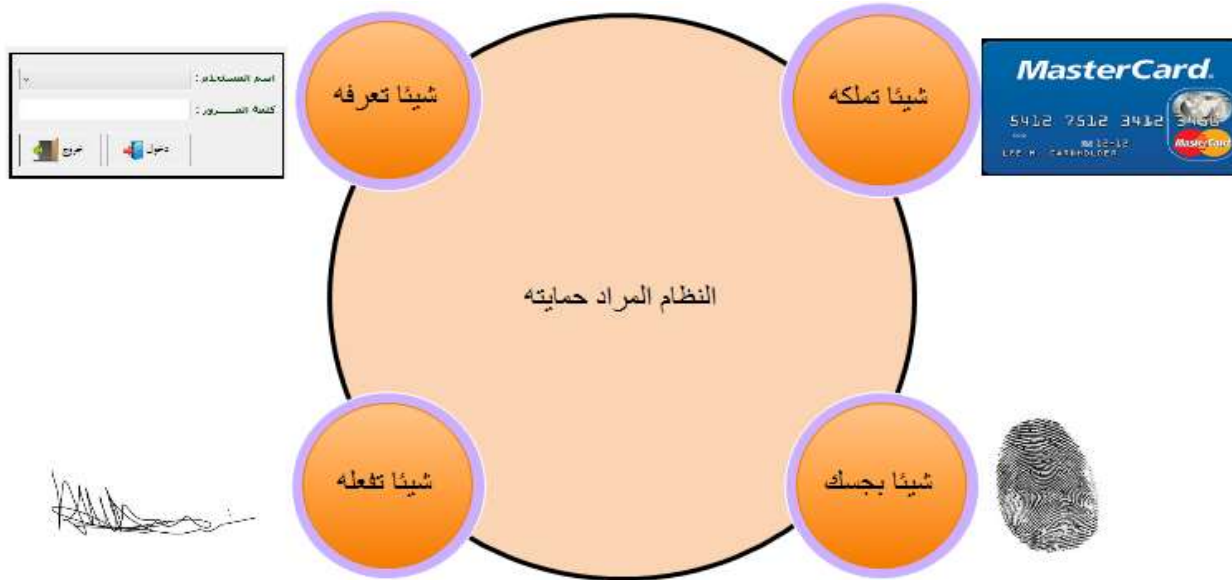
يحاول المستخدم  
الولوج للنظام  
مستخدماً كلمة  
سر، إذا نجحت  
المصادقة ينتقل  
بعدها إلى مرحلة  
التفويض ليعرف  
ما هي الموارد  
المسموح له  
بالوصول إليها،  
تتم متابعته في  
كل المراحل



# نظم التحكم بالوصول - المصادقة

المصادقة هي التحقق من هوية المستخدمين. يمكن تقسيم طرق المصادقة إلى:

1. شيئا تعرفه: كلمة المرور واسم المستخدم،
2. شيئا تملكه: بطاقة الصراف وبطاقة الفيزا وأيضا مفتاح الفوب
3. شيئا تفعله: مثل التوقيع أو الصوت.
4. شيئا بجسدك: مثل بصمة العين وبصمة الأصابع.



# نظم التحكم بالوصول - المنح

- يسمى أيضا التفويض authorization. بعد عملية المصادقة التي تتم على المدخل الرئيسي للنظام تأتي المرحلة الثانية وهي مرحلة التفويض وفيها يتم إعطاء أو منح الصلاحيات داخل النظام.
- يتم تعريف الموارد (المستخدمين، البرامج، العمليات، ..) وتعريف نوعية الوصول إليها (قراءة، كتابة، حذف، ...).
- على سبيل المثال بعد عملية المصادقة لدخول البوابة الرئيسية لنادي رياضي يتم بداخل النادي منح الصلاحيات لدخول أماكن معينة (ملعب التنس مثلا) ومنع دخول أماكن أخرى كأن يمنع الرجال من دخول حمام السباحة للسيدات.
- ليس معنى وجود صلاحيات الولوج للنظام، أن المستخدم يستطيع الوصول لكل شيء داخل النظام

# نظم التحكم بالوصول - المتابعة

- بعد المصادقة على دخول المستخدم من البوابة الرئيسية للنظام ومن ثم منحه بعض الصلاحيات للوصول لموارد النظام، يتم متابعته ومراقبته والإشراف على ما يفعله.
- والمتابعة تعني تسجيل كل ما يقوم به المستخدم. مثلا تسجيل ما هي الموارد التي استخدمها؟ وكيف استخدمها (كتابة، تعديل، حذف، ...). والمدة الزمنية التي استغرقها في استخدام ذلك المورد.

Date	Num	Description	Transfer	R	Deposit	Withdrawal	Balance
06/03/06		Transfere Money	Assets:Savings	y	100.00		679.79
06/03/06	106	ABC Hardware	-- Split Transaction --	y		100.00	579.79
14/03/06		Employers R Us	-- Split Transaction --	y	670.00		1,249.79
24/03/06		Transfer Money	Assets:Savings	y	500.00		1,749.79
25/03/06		ATM Withdrawal	Assets:Cash	y		100.00	1,649.79
28/03/06		Internet Subscription	Expenses:Internet	y		20.00	1,629.79
28/03/06	102	Light Company	Expenses:Electricity	y		78.00	1,551.79
28/03/06	103	Phane Company	Expenses:Phone	y		45.00	1,506.79
28/03/06	104	April Rent	Expenses:Rent	y		350.00	1,156.79
31/03/06		Service Charge	Expenses:Service Charge	y		5.00	1,151.79
28/04/06		May Rent	Expenses:Rent	n		350.00	801.79
05/05/06		Partial Payment of Visa Bill	Liabilities:Visa	n		300.00	501.79

# المصادقة – طرق المصادقة

طرق المصادقة هي :

- المصادقة بكلمة المرور
- المصادقة بالبطاقات
- المصادقة بالسمات الحيوية.



**المصادقة بكلمة المرور:** تستخدم كلمة المرور بالاقتران مع اسم المستخدم. واسم المستخدم أو ID لكل مستخدم يحدد هوية كل مستخدم ليتم الرجوع إليه واسترجاع الأحداث الخاصة به بعد عملية المتابعة.

يعيب المصادقة بكلمة المرور انه يمكن الهجوم على كلمة المرور بهجمة القاموس أو البحث الغاشم أو الاستيلاء على الحاسب أو التصنت على الشبكة. حتى بعد عمل هاش لها يمكن الهجوم عليها بهجمة جدول قوس قزح (تفاصيل أكثر في فصل التشفير). يستخدم التمليح لزيادة الحماية.



# المصادقة – كلمة المرور

مميزات الهاش مع التمليح لكلمات المرور: يتميز الهاش بالمميزات التالية والتي من خلالها نستطيع عرقلة المهاجمين بهجومهم ضد كلمة السر باستخدام القواميس :

- منع تخزين كلمات مرور متشابهة على نفس ملف كلمات السر. وبالتالي يمكن لمستخدمين مختلفين استخدام نفس كلمة المرور، وستظهر في ملف كلمات المرور في صورة أكواد هاش مختلفة.
- عرقلة المهاجمين المستخدمين لهجوم التخمين سواء الغاشم أو القاموس، حيث أن إضافة ملح للهاش بمقدار س بت سيزيد من محاولات التخمين بمقدار  $2^s$ .
- يستحيل معرفة ما إذا كان المستخدم يستعمل نفس كلمة المرور على أكثر من نظام. وبالتالي عرقلة هجوم إعادة تدوير كلمات المرور.



## تمرين عملي – إنشاء مستخدمين في ويندوز

– Open the User Account Tool

**Create an Account •**

**Password Protect the Account •**

**Change the Account Type •**

**Delete the Account •**

Show the created account in MyPC-> Manage •

# المصادقة – البطاقات



البطاقات الممغنطة

قارئ البطاقات الذكية

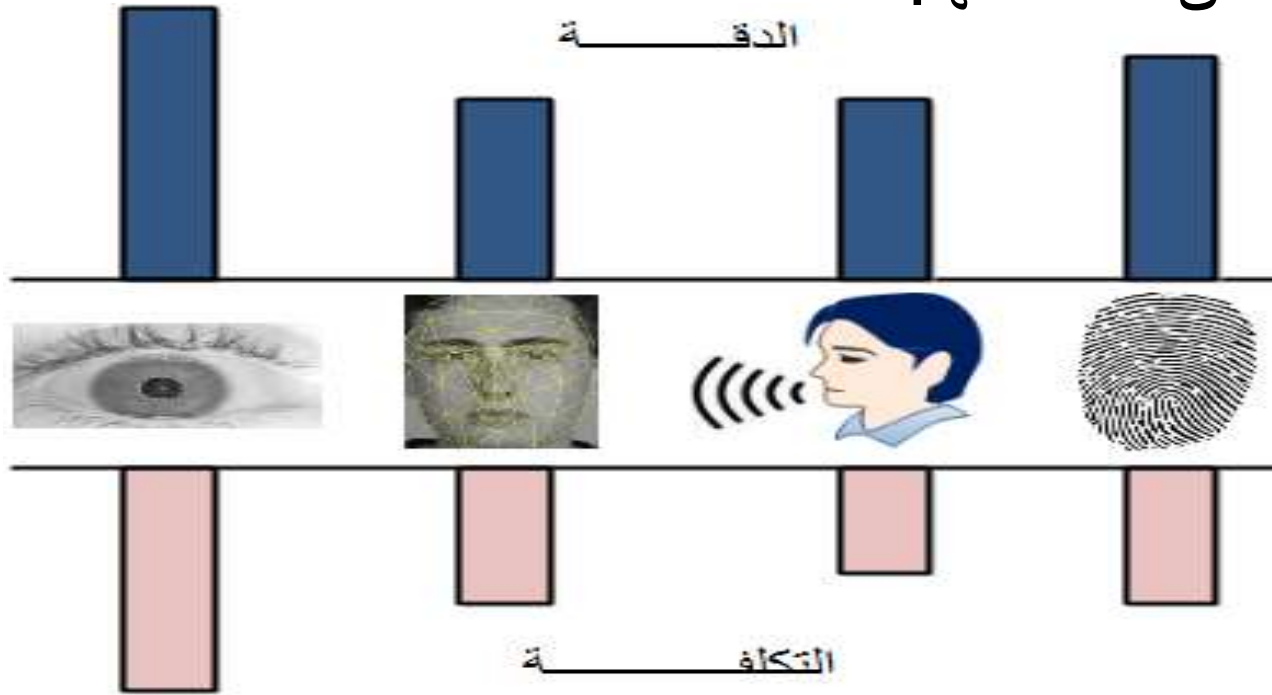
تستخدم بطاقة الصراف في سحب أو إيداع الأموال في ماكينة الصراف. وتستخدم بطاقة الائتمان في البيع والشراء على الانترنت. وأشهر أنواع البطاقات هي البطاقة الممغنطة والبطاقات الذكية:

**البطاقات الممغنطة** تقوم بتخزين البيانات فقط ولا تقوم بمعالجتها. وتحتوي على شريحة ذاكرة داخلية. من أمثلتها بطاقات الصراف ATM وبطاقات غرف الفنادق. يمكن الدمج بين رمز المرور والبطاقة بالمصادقة ذات عاملين

**البطاقات الذكية smart cards:** لها شريحة إلكترونية مدمجة. والشريحة بغرض المعالجة والتخزين وحماية البيانات. البطاقات الذكية تقوم بتخزين المعلومات الخاصة مثل أرقام الحسابات البنكية، رقم التعريف الشخصي، السجلات الطبية و البصمات الرقمية. توفر البطاقات الذكية نظام تشفير ومصادقة لحفظ البيانات آمنة.

# المصادقة – السمات الحيوية

من أفضل أنواع المصادقة هو استخدام صفة حيوية من صفات الشخص،  
الصفات الحيوية التالية يمكن استخدامها:



- بصمة الأصابع
- بصمة الصوت
- سمات الوجه
- بصمة العين

الأعلى دقة هو بصمة العين. والأقل دقة هو بصمة الصوت والوجه.  
والأعلى تكلفة هو بصمة العين والأقل تكلفة هو بصمة الصوت

# المنح ( التفويض )

التفويض يعني منع استخدام موارد النظام إلا بتصريح من مدير النظام. يقوم مدير النظام بإعطاء التصاريح بسياسات التفويض التالية:

- التحكم التقديري بالوصول (داك): Discretionary Access Control (DAC)
- التحكم الإلزامي بالوصول (ماك) Mandatory Access Control (MAC)
- التحكم بالوصول بناء على القواعد (قرباك)
- التحكم بالوصول بناء على الأدوار (أرباك) Role Based Access Control (RBAC)

# المنح - التحكم التقديرى بالوصول (داك)

يتم التحكم بالوصول حسب تقدير وتصرف مالك الكائن. إذا كان لمالك الكائن صلاحيات وصول معينة يمكنه إعطاء هذه الصلاحيات ونقلها لفاعل آخر.

من الطرق المشهورة لتحقيق ذلك هو استخدام مصفوفة الوصول access matrix. ويمكن تحويل مصفوفة الوصول إلى قائمة التحكم بالوصول (ACL) Access Control List أو العكس.

## قائمة التحكم بالوصول ACL:

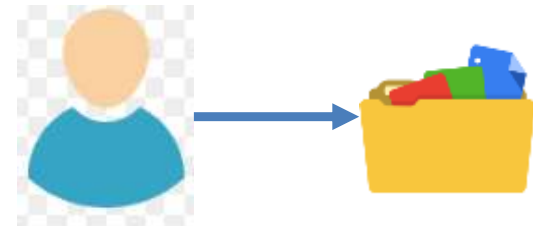
- F1 >> Allow any R, Allow U1 W
- F2 >> Deny U1, Allow U2 R, O
- F3 >> Deny U2, Allow U1 W

ملف 3 F3	ملف 2 F2	ملف 1 F1	
W		R, W	مستخدم (U1)1
	R, O	R	مستخدم (U2)2

R: Read القراءة

W: Write الكتابة

O: Own المالك



# المنح - التحكم التقديرى بالوصول (داك)

يمكن إضافة بعض القيود للصلاحيات كمنح الصلاحيات بقيد زماني او مكاني:

**القيد الزماني Temporal** يتم منح الصلاحيات للمستخدمين في أوقات معينة ومنعها عنهم في أوقات أخرى. على سبيل المثال يمكن منح الصلاحيات للموظفين أثناء ساعات العمل الرسمية ومنعها عنهم في الأوقات الأخرى.

**القيد المكاني Spatial** ويعني منح الصلاحيات للمستخدم في أماكن ومنعها عنه في أماكن أخرى. على سبيل المثال منح الصلاحيات لطلاب جامعة طيبة فرع ينبع إذا حاول الطالب الدخول للنظام من محافظة ينبع، ومنع الصلاحيات عنه في حالة دخوله للنظام من مدن أخرى والتي توجد فيها أفرع جامعة طيبة مثل خيبر أو بدر.

# المنح - التحكم الإلزامي بالوصول (ماك)

يقيد الأفعال التي يقوم بها **الفاعل** تجاه أي **كائن**. الفاعل يمكن أن يكون مستخدم أو إجراء. والكائن يمكن أن يكون ملف أو منفذ

- تستخدم المؤسسات النظام الإلزامي عندما يوجد عدة مستويات للتصنيفات الأمنية. فكل كائن له علامة وكل فاعل له تصريح. والنظام الإلزامي يحكم وصول الفاعل بناء على التصنيف الأمني للكائن ولتصريح المستخدم.

- على سبيل المثال، نظام التصنيف الأمني الحربي يصنف المستندات عموماً لسري وسري للغاية. فإذا كان ملف له العلامة سري للغاية، فإن الأشخاص (الفاعلون) الذين يمكنهم عرض هذا الملف هم من يملكون تصريح من النوع سري للغاية



- فاعل ذو تصريح سري للغاية لا يمكنه إرسال ملف سري للغاية لمستخدم يحمل تصريح سري فقط

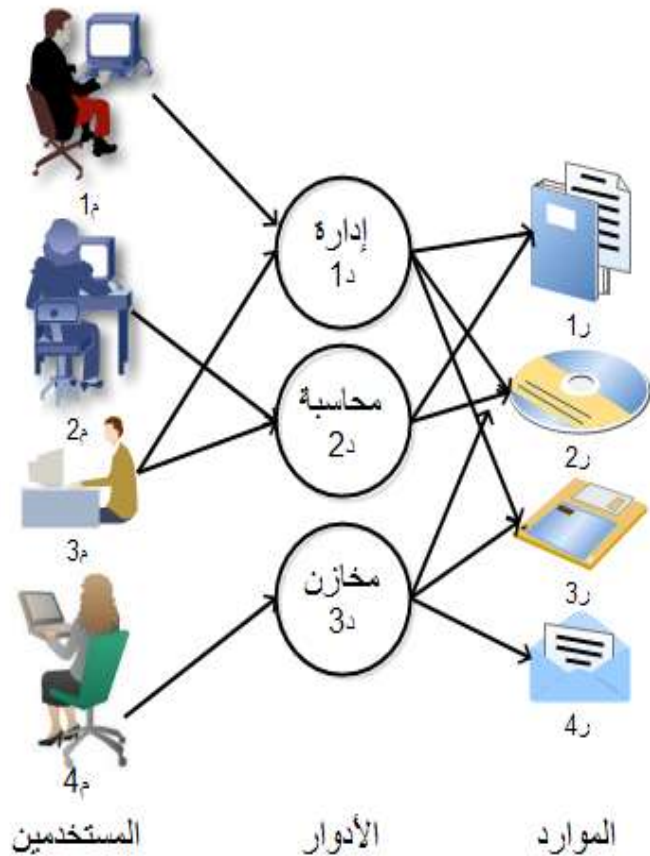


# المنح - التحكم بالوصول بناء على الأدوار (أرباك)

- يعتمد على دور أو وظيفة الفاعل داخل الشركة. الأدوار هي المهام الوظيفية بداخل المؤسسات،
- يساعد في بناء إدارة أمنية ناجحة في المؤسسات الكبرى والتي بها مئات المستخدمين وآلاف الصلاحيات المحتملة
- تستخدم في التطبيقات فنظام قواعد البيانات SQL Server ونظام أوراكل يستخدمان نظام أرباك لعمل التفويض.
- لا يتم منح الصلاحيات للمستخدمين بشكل مباشر كما في نظام داك.
- ولكن توجد قائمة الأدوار التي تفصل المستخدمين عن الموارد.
- لا توضع الصلاحيات على الموارد ولكن توضع على الأدوار



# المنح - التحكم بالوصول بناء على الأدوار (أرباك)



مصفوفة الوصول

	4ر	3ر	2ر	1ر	
1د		R,W	R,W	R	
2د			W	R	
3د	R,W	R	R,W		

تعيين أدوار المستخدمين

	3د	2د	1د	
1م			✓	
2م		✓		
3م		✓	✓	
4م	✓			

يتم إعطاء الصلاحيات للأدوار كما هو موضح بـ "مصفوفة الوصول" ثم يتم إضافة/إزالة المستخدم عن طريق مصفوفة "تعيين الأدوار" للمستخدمين. فإذا انضم المستخدم للدور، أخذ كل صلاحياته.



# تمرين عملي – إدارة المستخدمين في ويندوز

- **Access Local Users and Groups Manager.**
  - Create new users, change password
- **Verify user and group permissions. (if you member of “Users” group will not be able to create users**
  - You can run most applications as allowed by the permissions for a member of the Users group.
    - **Create new groups. Add users to them**
      - **Assign group permissions to folders.**
    - **Verify and modify folder permissions.**
      - **Disable a user account.**
      - **Clean up.**

# المنح - النماذج المرجعية لنظام أرباك

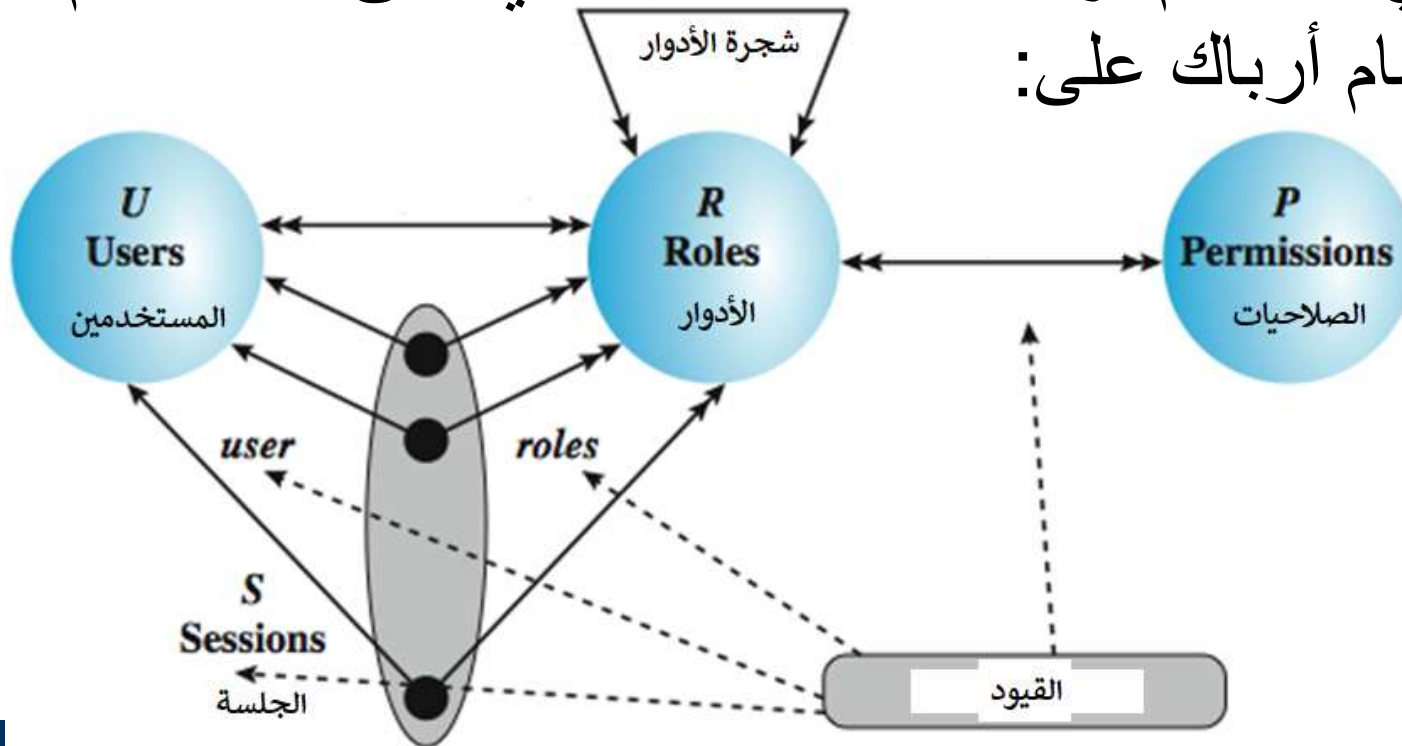
توجد ثلاث نماذج مرجعية لـ أرباك، نموذج واحد أساسي وهو النموذج الذي تبنى عليه النماذج الأخرى، ونموذجين إضافيين اختياريين يمكن استخدامهما أو تركهما، والنماذج المرجعية هي:

- النموذج المرجعي الأساسي
- النموذج المرجعي الإضافي - شجرة الأدوار
- النموذج المرجعي الإضافي - القيود

# المنح - النماذج المرجعية لنظام أرباك

النموذج المرجعي الأساسي: إذا أراد مدير النظام بناء نظام أرباك فإن عليه أولاً أن يبني نموذج مرجعي أساسي. النموذج المرجعي الأساسي يكون في كل نظم أرباك لأنه الأساس الذي يبنى عليه نظام أرباك. يحتوى نظام أرباك على:

- المستخدمين
- الأدوار
- الصلاحيات
- الجلسات.

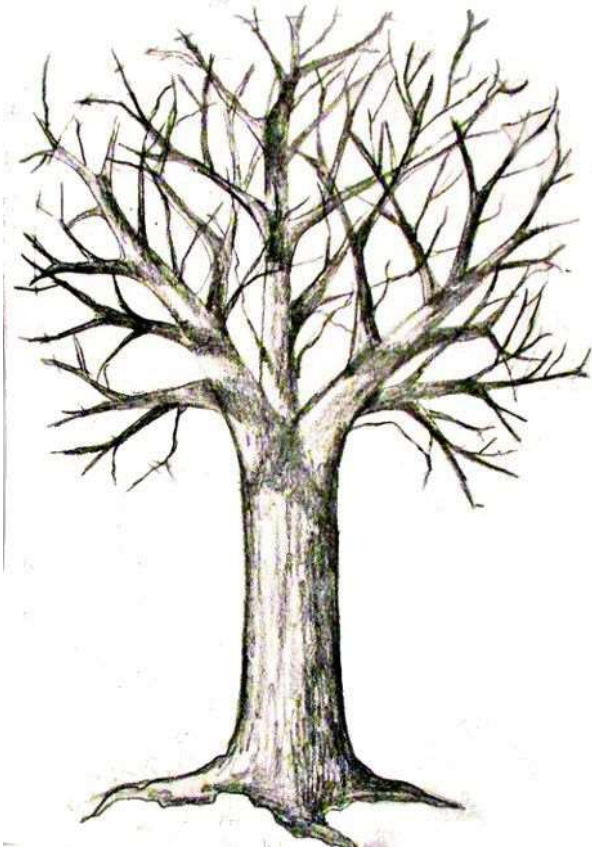


# المنح - النماذج المرجعية لنظام أرباك

## مكونات النموذج المرجعي الأساسي

- المستخدمين: هم الفاعلون الذين لديهم صلاحيات النظام.
- الأدوار: وهي الوظيفة المؤسسية التي تكون في الشركة، مثل دور مدير ومحاسب وعامل نظافة وأمين مخزن ومساعد مدير.
- الصلاحيات: تحدد شكل الوصول للكائنات داخل النظام،
- الجلسات: هي عبارة عن المجموعة الفرعية من الأدوار (التي تحتوي على الصلاحيات) التي يتم إعطاؤها للمستخدم في الوقت الفعلي أو أثناء التشغيل. ويتم إعطاء هذه المجموعة الفرعية من الأدوار للمستخدم للقيام بمهمة معينة، فإذا انتهت المهمة يتم إنهاء الجلسة وسحب الصلاحيات منه مرة أخرى.

# المنح - النماذج المرجعية لنظام أرباك



## النموذج المرجعي الإضافي - شجرة الأدوار

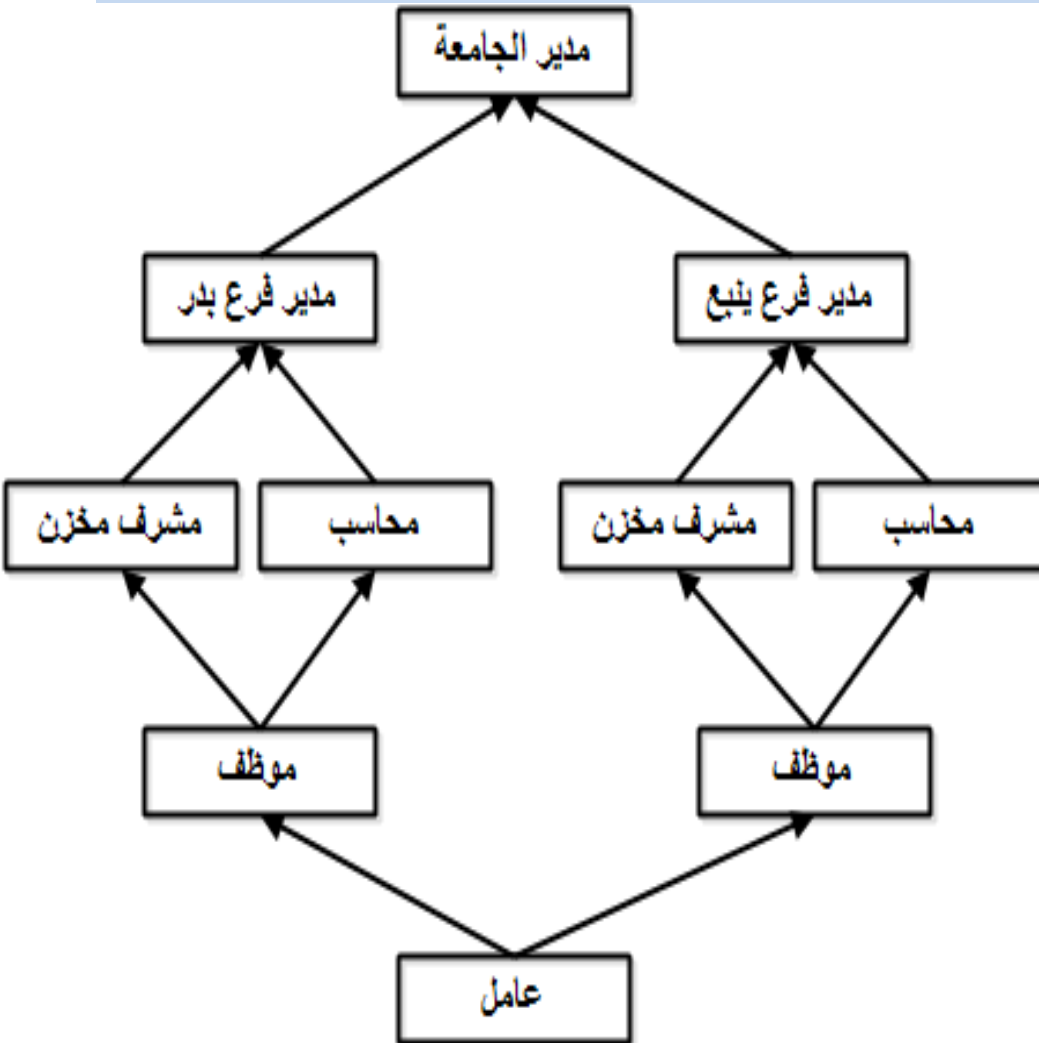
- ممكن زيادة كفاءة النظام المرجعي الأساسي بإضافة النظام المرجعي الشجري (الشكل الهرمي)
- يقسم الأدوار بالمؤسسة على شكل شجرة تسمى شجرة الأدوار يحتوي جذرها على الأدوار الدنيا في المؤسسة كعامل النظافة و السائقين. وأطرافها تتكون من عدة مستويات مرتبة حسب الدور الوظيفي

# المنح - النماذج المرجعية لنظام أرباك

## شجرة الأدوار

الصلاحيات الأعلى على  
أطراف الشجرة لأعلى  
والصلاحيات الأقل توجد في  
جذور الشجرة، المستويات  
الأعلى ترث صلاحيات  
المستويات الأقل.

أقل الأدوار في الصلاحية هو  
دور "العامل" وأعلى الأدوار  
في الصلاحية هو دور "مدير  
الجامعة"





# المنح - النماذج المرجعية لنظام أرباك



النموذج المرجعي الإضافي - القيود  
يتم إضافة نموذج القيود للنموذج  
المرجعي الأساسي عند الحاجة  
لفرض سياسات وقيود إدارية في  
المؤسسة. ويعرف بعض  
العلاقات بين الأدوار أو شروط  
للوصول للأدوار. والقيود هي:  
الأدوار المنفصلة، رتبة الدور، الدور  
المتطلب، مبدأ أقل الحاجة والقيود  
الزمني والمكاني

# المنح - النماذج المرجعية لنظام أرباك

## النموذج المرجعي الإضافي - القيود

1. الأدوار المنفصلة: تعني أن تتفصل الأدوار عن بعضها فلا يمكن لمستخدم واحد أن يوجد في دورين في نفس الوقت. ويمكن أيضا تطبيق قيد الأدوار المنفصلة على الصلاحيات. فلا تعطي صلاحية معينة إلا لدور واحد فقط. بمعنى أنه لا يمكن لصلاحية محددة (كالتعديل في قاعدة بيانات الموظفين مثلا) أن توجد في دورين مختلفين. الحقيقة أن الانفصال المنطقي (XOR) موجود في نظم عدة. ففي نظام المخازن فإنه من غير المنطقي أن توجد قطعة فيزيائية مثل الطابعة في مكتبين مختلفين في نفس الوقت.

2. رتبة الدور: رتبة الدور تعرف أقصى عدد للمستخدمين الملتحقين بدور معين. على سبيل المثال يمكن عمل قيد بأن أقصى عدد للمستخدمين في دور واحد يكون 3 مستخدمين.

# المنح - النماذج المرجعية لنظام أرباك

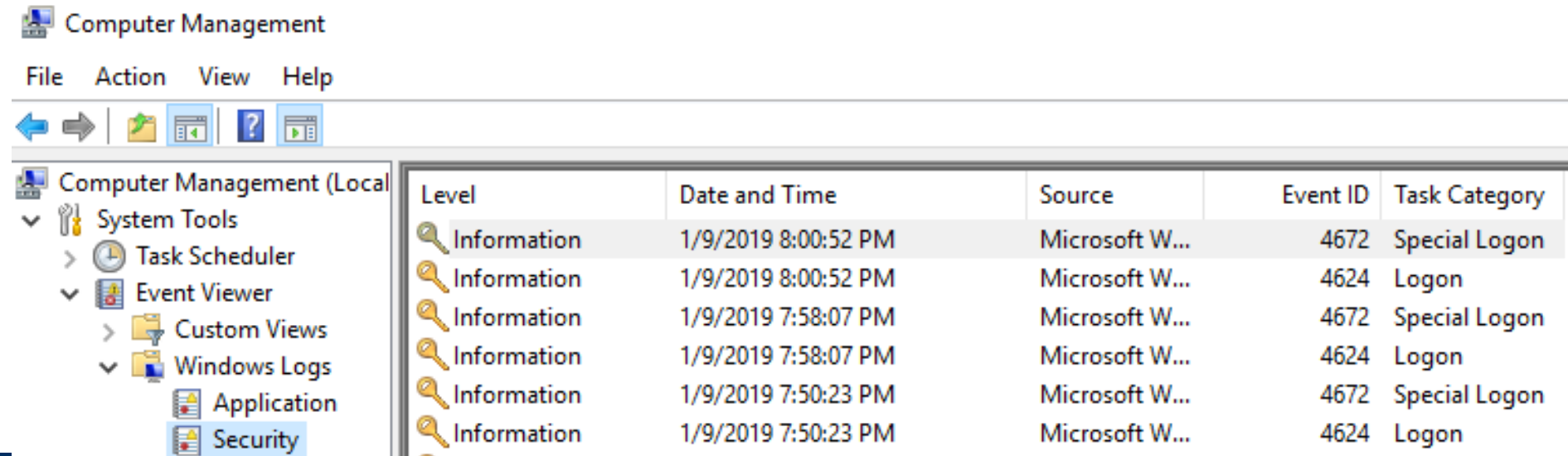
## النموذج المرجعي الإضافي - القيود

3. الدور المتطلب: وهي مثل المتطلب السابق للمواد في الجامعة. ويعني هذا القيد أن المستخدم لا يمكن أن يلتحق بدور معين إلا إذا كان ملتحقاً بالأصل بدور آخر محدد.
4. مبدأ أقل الحاجة: ويعني تقليل الصلاحيات للدور بحيث تكون أقل ما يمكن. يمكن تطبيق ذلك القيد أثناء بناء النظام أو عند عمل جلسة.
5. القيد الزماني والمكاني: يطبق القيد الزماني والمكاني على الدور. على سبيل المثال، في القيد الزماني يمكن تفعيل صلاحيات الدور في الفترة من 8 صباحاً حتى 4 بعد الظهر وهو وقت العمل الرسمي وتعطيها في باقي اليوم وفي إجازة نهاية الأسبوع. وفي القيد المكاني يمكن ربط الأدوار بمكان جغرافي محدد.

# المتابعة

المتابعة أو المسائلة تعطي مسئولية حدث معين مثل التعديل في النظام وتربطه بشخص ما أو عملية ما وتجمع تلك المعلومات ثم تعطي تقريراً يسمى تقرير استخدام البيانات.

والبيانات المجمعة تحتوي على سجل الأحداث بالوقت والتاريخ لمستخدم بعينه سواء تم الحدث بنجاح أم فشل، وأيضا ما استخدمه من موارد لعمل ذلك الحدث.



The screenshot shows the Windows Event Viewer application. The left pane displays the 'Computer Management (Local)' tree with 'System Tools' expanded, showing 'Task Scheduler', 'Event Viewer', 'Custom Views', 'Windows Logs', 'Application', and 'Security'. The right pane shows a list of events with the following columns: Level, Date and Time, Source, Event ID, and Task Category.

Level	Date and Time	Source	Event ID	Task Category
Information	1/9/2019 8:00:52 PM	Microsoft W...	4672	Special Logon
Information	1/9/2019 8:00:52 PM	Microsoft W...	4624	Logon
Information	1/9/2019 7:58:07 PM	Microsoft W...	4672	Special Logon
Information	1/9/2019 7:58:07 PM	Microsoft W...	4624	Logon
Information	1/9/2019 7:50:23 PM	Microsoft W...	4672	Special Logon
Information	1/9/2019 7:50:23 PM	Microsoft W...	4624	Logon

# المتابعة - إنشاء المتابعة

- يوفر ملف سجل الأحداث (لوج Log) معلومات تفصيلية بناء على المتغيرات المختارة. على سبيل المثال، تقوم المؤسسة بالاهتمام بعملية دخول النظام بتسجيل عدد مرات الدخول الناجحة والفاشلة
- الدخول الفاشل يوضح في غالب الأحيان أن هناك سارقا يحاول اختراق الحساب.
- عمليات الدخول الناجحة تعرف المؤسسة من المستخدمين الذين استخدموا الموارد ومتى تم الاستخدام. فهل يكون من الطبيعي أن يحاول المستخدم صاحب الصلاحيات الولوج لشبكة النظام الساعة 3 بعد منتصف الليل؟



# الأسئلة