یا ذاالامن والامان

امنیت داده و شبکه

امنیت سیستم – کنترل دسترسی

مرتضی امینی - سیدمهدی خرازی

نیم‌سال اول ۱۴۰۴-۱۴۰۳

فهرست مطالب

- مقدمه
- مدل‌های کنترل دسترسی اختیاری
- مدل‌های کنترل دسترسی اجباری
- مدل‌های کنترل دسترسی نقش-مبنا

تعاریف

- **خط‌مشی کنترل دسترسی:** چه عامل‌هایی اجازه انجام چه اعمالی را بر روی چه اشیایی دارند و یا ندارند.
- در قالب مجموعه‌ای قاعده دسترسی بیان می‌گردد.
  - علی اجازه خواندن و تغییر اطلاعات حقوق افراد را دارد.
  - کارمندان عادی اجازه خواندن قراردادهای شرکت را ندارند.
  - سیستم‌های درون سازمان (به غیر از سرورها) اجازه برقراری ارتباط با شبکه‌های بیرونی را ندارند.

تعاریف

مدل کنترل دسترسی (مجازشماری)

- تعریف: انتزاعی از خط‌مشی‌های امنیتی و کنترل دسترسی
- بیانگر ساختار داده‌ای و زبان توصیف خط‌مشی‌های کنترل دسترسی و رویه کنترل دسترسی
- نیازمندی‌ها یا **خط‌مشی‌های امنیتی** در کاربردهای مختلف، متفاوت است، لذا نوع **مدل‌های امنیتی یا کنترل دسترسی** حاصله نیز متفاوت است.

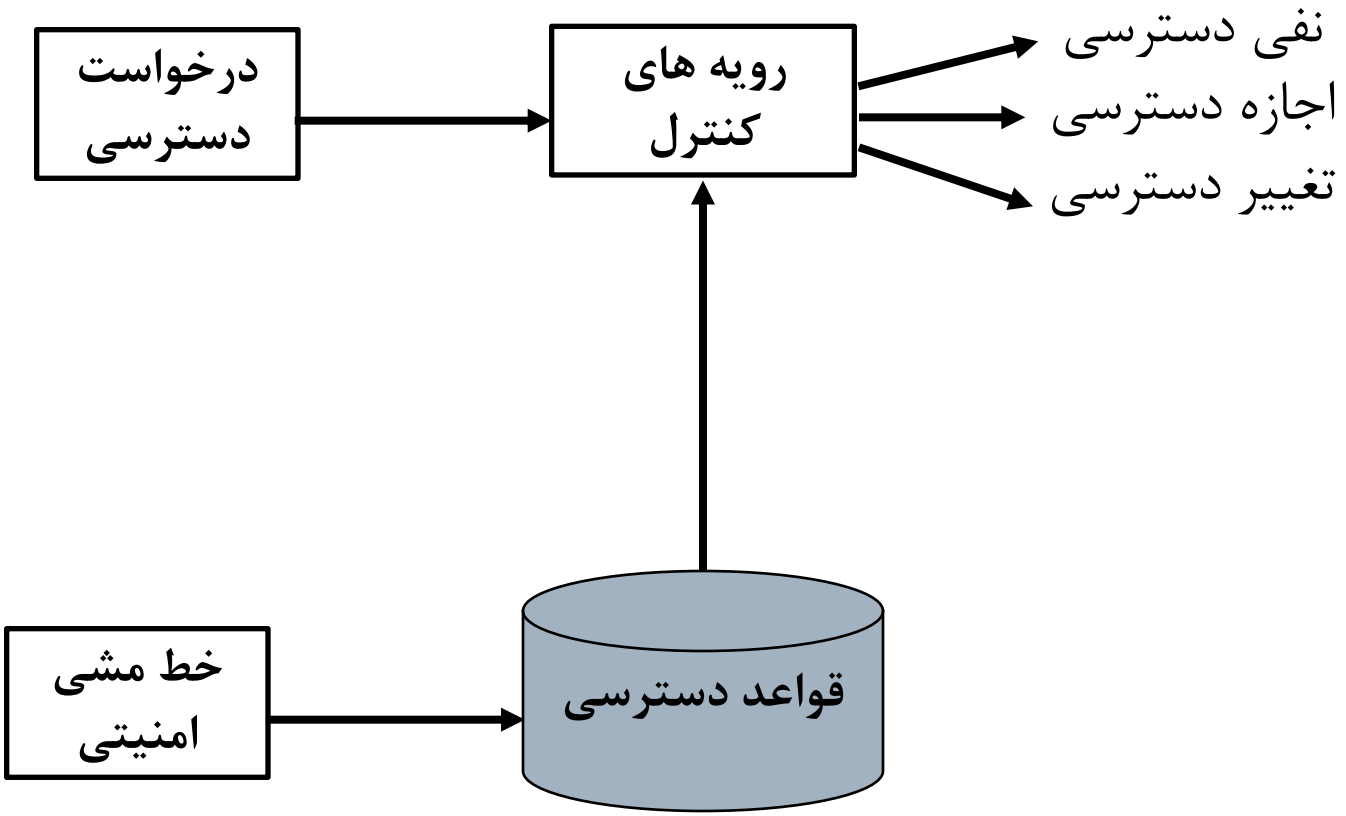
مکانیزمِ (اِعمال) کنترل دسترسی

- تعریف: روش و سیستم اِعمال کنترل دسترسی بر اساس خط‌مشی‌های توصیف شده
- مبتنی است بر یک مدل کنترل دسترسی

عناصر اصلی در کنترل دسترسی

- موجودیت‌های اصلی دخیل در کنترل دسترسی:
  - عامل (Subject): هر آنکه متقاضی دسترسی است.
    - عامل انسانی، عامل ماشینی، پردازه، وب سرویس و . . .
  - شیئ یا منبع (Object or Resource): هر آنچه مورد دسترسی قرار می‌گیرد.
    - فایل، جدول پایگاه داده، پردازه، پردازنده، . . .
  - عمل (Action): عملی که توسط عامل بر روی شیئ یا منبع انجام می‌شود.
    - خواندن، نوشتن، تغییر، حذف، چاپ، . . .
- عامل عنصری فعال (Active) و شیئ عنصری منفعل (Passive) است.
  - یک عنصر می‌تواند هم نقش عامل را داشته باشد و هم نقش شیئ.
    - مثال: پردازه در سیستم عامل، وب‌سرویس در محیط وب

مکانیزم کنترل دسترسی



انواع خط‌مشی‌ها و مدل‌های کنترل دسترسی

- بر اساس معیارهای مختلفی می‌توان مدل‌ها را دسته‌بندی کرد.
- انواع مدل‌های کنترل دسترسی بر حسب نحوه انتساب مجوزها:
  - مدل کنترل دسترسی اختیاری (DAC)
  - مدل کنترل دسترسی اجباری (MAC)
  - مدل کنترل دسترسی نقش-مبنا (RBAC)

فهرست مطالب

- مقدمه
- **مدل‌های کنترل دسترسی اختیاری**
- مدل‌های کنترل دسترسی اجباری
- مدل‌های کنترل دسترسی نقش-مبنا

مدل‌های کنترل دسترسی اختیاری

- خصوصیات اصلی مدل‌های کنترل دسترسی اختیاری:
  - **مبتنی بر شناسه** و نیاز به شناسایی کاربر و **احراز هویت** آن
    - *مثال: حسن اجازه خواندن فایل x.doc را دارد.*
    - *مثال: علی اجازه تغییر جدول y را در پایگاه داده‌ها ندارد.*
  - اعطای مجوزهای دسترسی به منابع، در **اختیار مالک** است.
    - *مثال: مالک x.doc مجوز دسترسی خواندن را به حسن می‌دهد.*

مدل‌های کنترل دسترسی اختیاری

- مدل‌های ماتریس-مبنا از انواع معروف مدلهای اختیاری هستند.
  - هر سطر مربوط به یک عامل و هر ستون مربوط به یک شیئ است.
  - هر درایه ماتریس، مجوزهای دسترسی یک عامل را به یک شیئ نشان می‌دهد.

Rights	Objects			
Subjects		O_1	O_2	O_3
	S_1	+r	-r, +w	+r, +w
	S_2	-w	+w	+r, -w

لیست قابلیت
C-List

لیست کنترل دسترسی
ACL

مدل‌های کنترل دسترسی اختیاری

- انواع مدل‌های کنترل دسترسی اختیاری بر حسب اینکه مجوز پیش‌فرض چه باشد:
  - **مدل‌های باز:** یک عامل به یک شیئ دسترسی دارد مگر آنکه خلاف آن در قواعد دسترسی بیان شده باشد.
  - **مدل‌های بسته:** یک عامل به یک شیئ دسترسی ندارد مگر آنکه در قواعد دسترسی، مجوز دسترسی به آن شیئ صادر شده باشد.

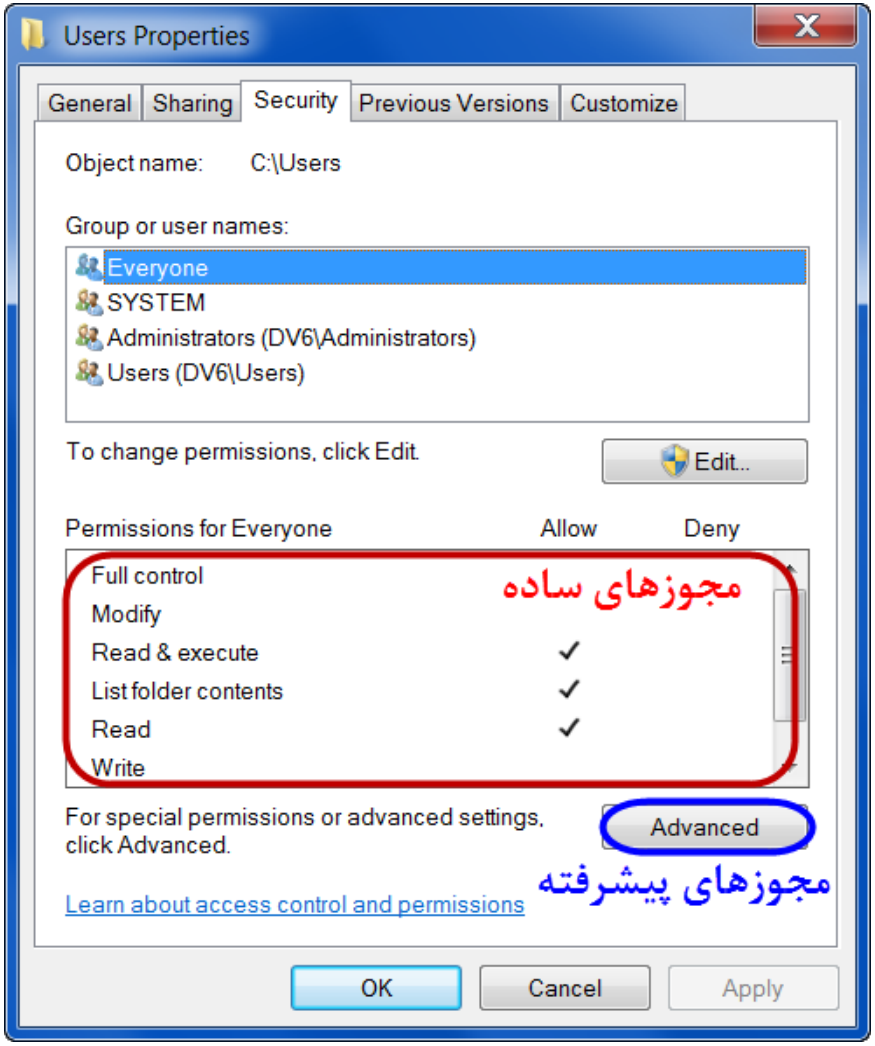
مکانیزم‌های کنترل دسترسی اختیاری

- پیاده‌سازی مکانیزم‌های کنترل دسترسی مبتنی بر مدل کنترل دسترسی اختیاری بر دو روش استوار است:
  - **مبتنی بر قابلیت (Capability based)**
    - مجوزهای هر عامل را خود عامل به صورت یک لیست از قابلیت‌ها یا مجوزها (C-List) در دست دارد و جهت دسترسی به منابع، آنها را ارائه می‌نماید.
    - *مثال: کنترل دسترسی به سرویس‌ها در کربروس (بلیط سرویس= قابلیت یا مجوز دسترسی به سرویس)*
  - **مبتنی بر لیست کنترل دسترسی (Access Control List)**
    - لیست عامل‌ها و مجوزهای آنها (ACL) در کنار هر شیئ یا منبع قرار می‌گیرد.
    - *مثال: پیاده‌سازی کنترل دسترسی در لینوکس*

مدل کنترل دسترسی اختیاری

- **مزایا:**
  - سادگی، انعطاف‌پذیری
- **معایب:**
  - عدم کنترل جریان اطلاعات و کانال‌های مخفی، عدم کنترل استنتاج
  - سختی مدیریت: مدیر با حجم زیادی از مجوزها و افراد سر و کار دارد.
- **کاربرد:**
  - سیستم‌های کاربردی تجاری که فاقد طبقه‌بندی اطلاعات هستند.
  - سیستم‌های متمرکز با کاربران شناخته شده محدود.

کنترل دسترسی اختیاری در ویندوز (۱)

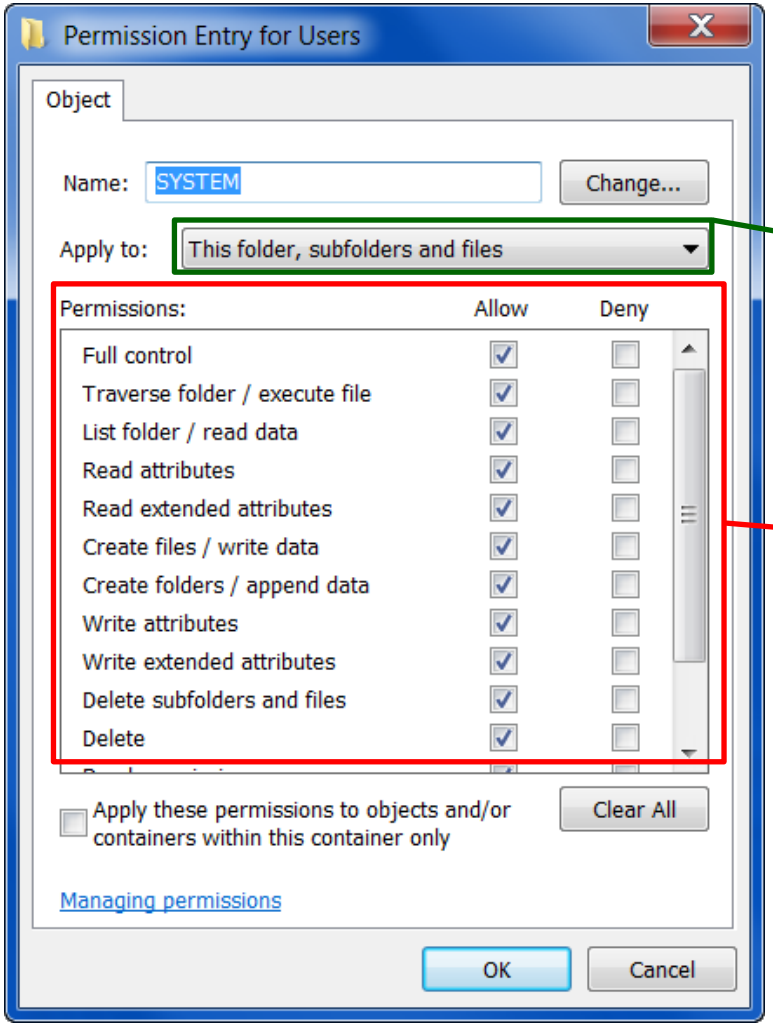


مجوزهای NTFS

- برای سادگی، به دو دسته تقسیم شده‌اند:
  - مجوزهای ساده
  - مجوزهای پیشرفته
- هریک از مجوزها می‌توانند اعطا شده یا منع شوند.

کنترل دسترسی اختیاری در ویندوز (۲)

مجوزهای پیشرفته NTFS

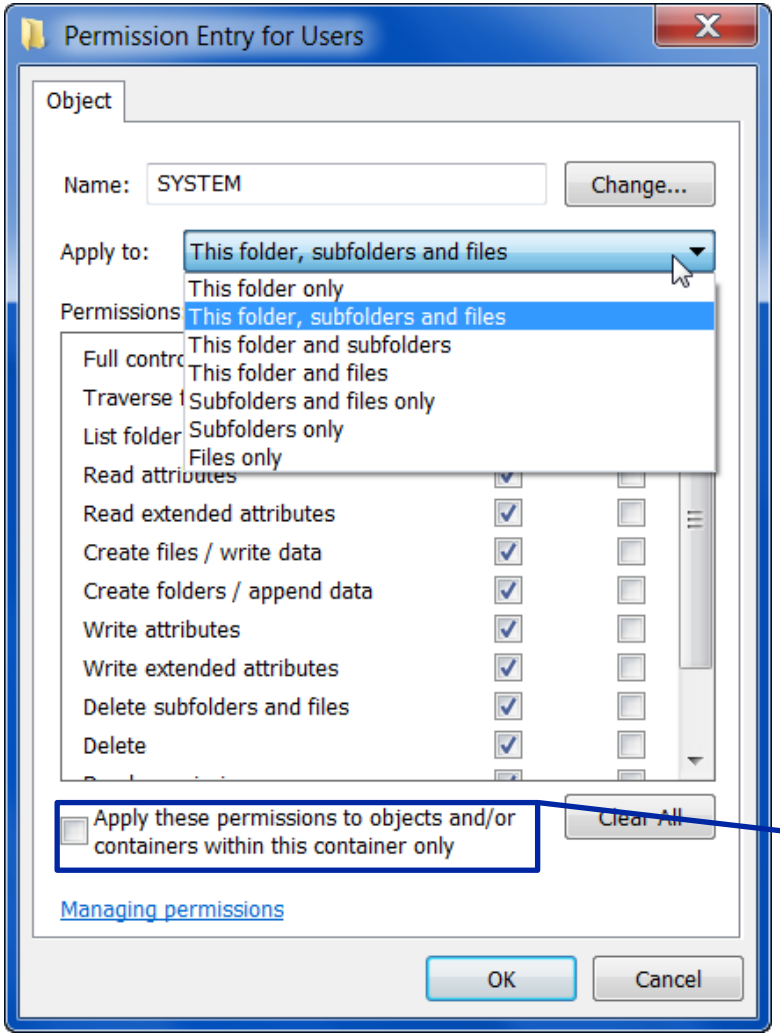


حوزه (**scope**) اعمال مجوز؛
شامل چگونگی وراثت مجوز

لیستی از ۱۳ مجوز ریزدانه
(+ ۱۴امین مجوز: **Full Control**)

کنترل دسترسی اختیاری در ویندوز (۳)

حوزه اِعمال مجوزها



مهم !

(توضیحات در اسلاید بعدی)

کنترل دسترسی اختیاری در ویندوز (۴)

حوزه اِعمال مجوزها

محل اعمال ← / نام حوزه ↓	پوشه جاری	زیرپوشه‌های داخل این پوشه (۱ سطح پایین‌تر)	فایلهای داخل این پوشه (۱ سطح پایین‌تر)	تمام زیرپوشه‌ها	تمام فایلها در تمام زیرپوشه‌ها
This folder only	×				
This folder, subfolders and files	×	×	×	×	×
This folder and subfolders	×	×		×	
This folder and files	×		×		×
Subfolders and files only		×	×	×	×
Subfolders only		×		×	
Files only			×		×

کنترل دسترسی اختیاری در ویندوز (۵)

حوزه اِعمال مجوزها

محل اعمال ← / نام حوزه ↓	پوشه جاری	زیرپوشه‌های داخل این پوشه (۱ سطح پایین‌تر)	فایلهای داخل این پوشه (۱ سطح پایین‌تر)	تمام زیرپوشه‌ها	تمام فایلها در تمام زیرپوشه‌ها
This folder only	×				
This folder, subfolders and files	×	×	×	×	×
This folder and subfolders	×	×		×	
This folder and files	×		×		×
Subfolders and files only		×	×	×	×
Subfolders only		×		×	
Files only			×		×

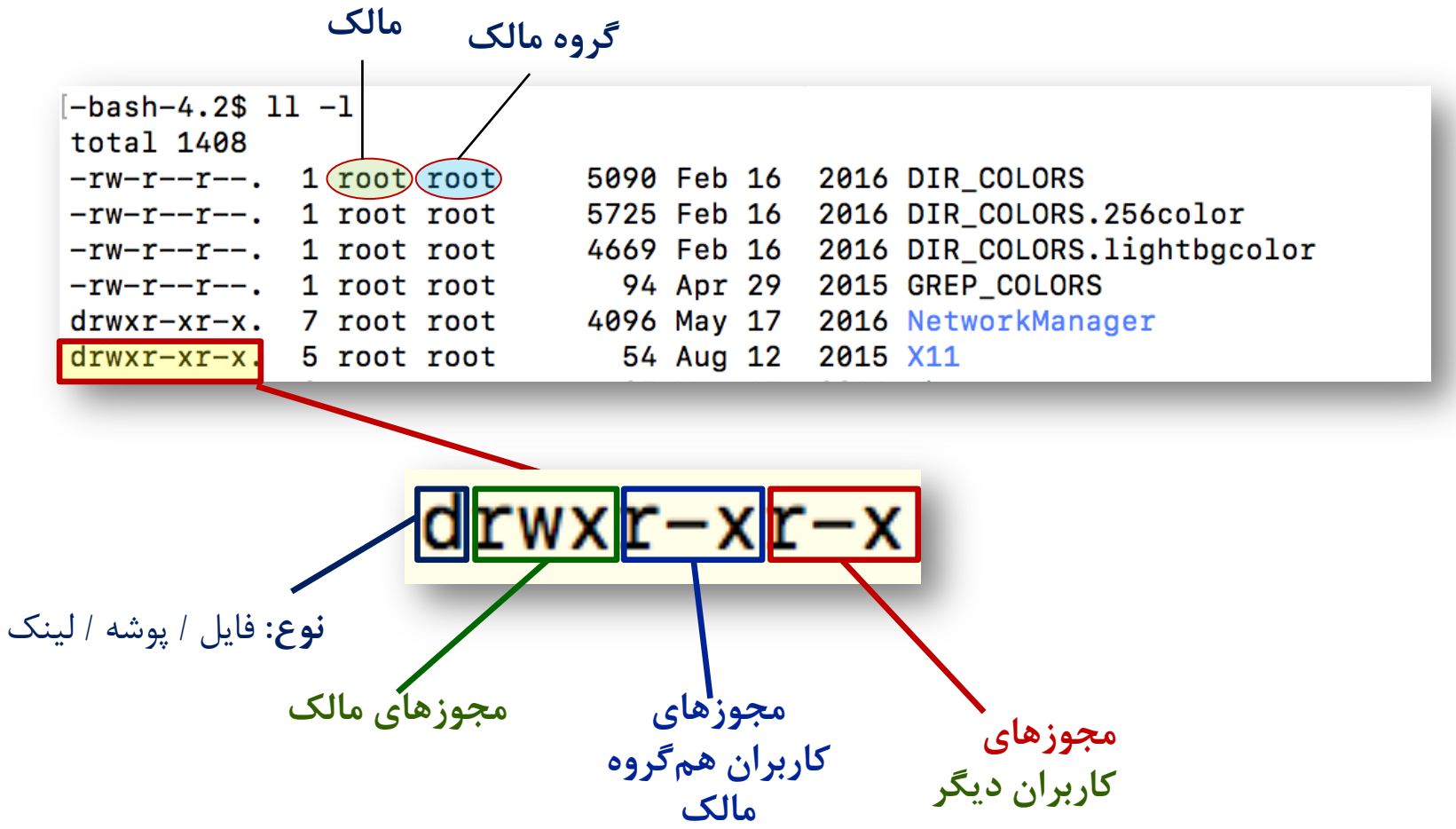
در صورتی که گزینه
Apply these permissions to objects and/or containers within this container only
انتخاب شده باشد، مجوزها به حوزه‌های مذکور در این دو ستون اعمال نمی‌شود.

کنترل دسترسی اختیاری در ویندوز (۶)

نگاشت بین مجوزهای ساده و پیشرفته NTFS

مجوز پیشرفته ↓ / مجوز ساده →	Write	Read	List folder contents	Read & execute	Modify	Full Control
Traverse folder/ execute file			×	×	×	×
List folder/read data		×	×	×	×	×
Read attributes		×	×	×	×	×
Read extended attributes		×	×	×	×	×
Create files/write data	×				×	×
Create folders/append data	×				×	×
Write attributes	×				×	×
Write extended attributes	×				×	×
Delete subfolders and files						×
Delete					×	×
Read permissions		×	×	×	×	×
Change permissions						×
Take ownership						×

کنترل دسترسی اختیاری در لینوکس (۱)



کنترل دسترسی اختیاری در لینوکس (۲)

```
-bash-4.2$ ll -l
total 1408
-rw-r--r--.  1 root root     5090 Feb 16  2016 DIR_COLORS
-rw-r--r--.  1 root root     5725 Feb 16  2016 DIR_COLORS.256color
-rw-r--r--.  1 root root     4669 Feb 16  2016 DIR_COLORS.lightbgcolor
-rw-r--r--.  1 root root       94 Apr 29  2015 GREP_COLORS
drwxr-xr-x.  7 root root     4096 May 17  2016 NetworkManager
drwxr-xr-x.  5 root root       54 Aug 12  2015 X11
```

مجوز	بر روی فایل	بر روی پوشه
r	خواندن	لیست کردن (با **ls**)
w	نوشتن	ایجاد/حذف/تغییر نام فایلها در پوشه
x	اجرا	برای ورود به پوشه (با **cd**) جهت دسترسی به فایلهای آن
-	عدم وجود مجوز	عدم وجود مجوز

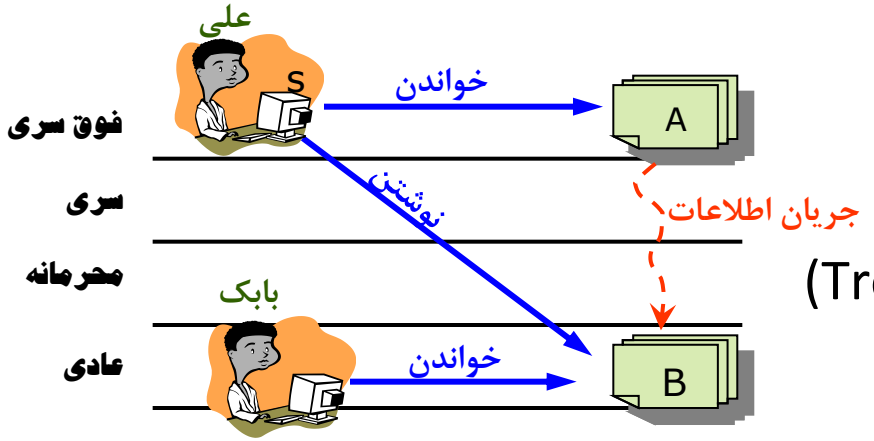
مطالعه بیشتر: مجوزهای پیشرفته SUID، SGID و Sticky Bit را در لینوکس مطالعه نمایید.

فهرست مطالب

- مقدمه
- مدل‌های کنترل دسترسی اختیاری
- **مدل‌های کنترل دسترسی اجباری**
- مدل‌های کنترل دسترسی نقش-مبنا

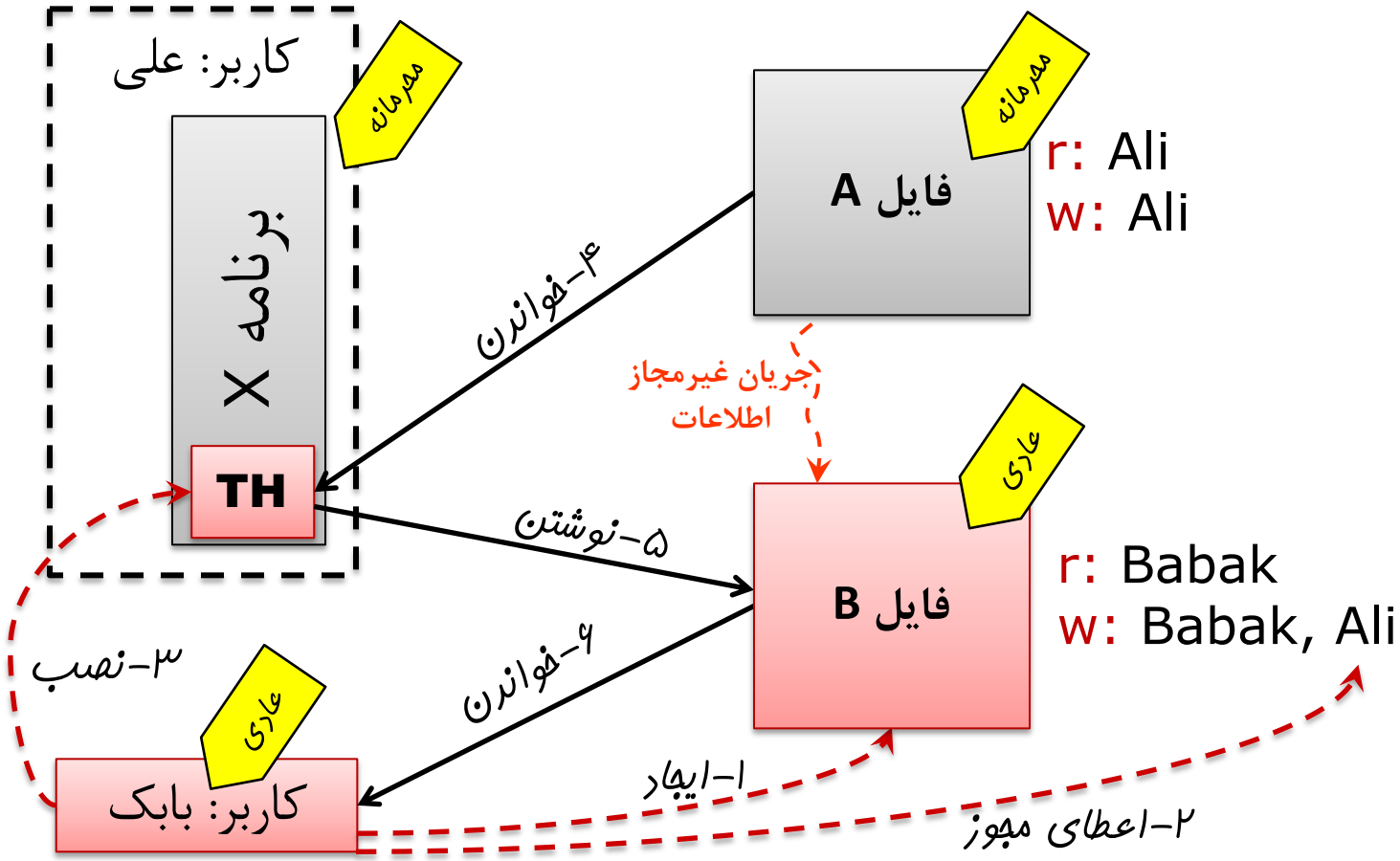
ضعف مدل کنترل دسترسی اختیاری

- عدم امکان کنترل انتشار اطلاعات توسط عامل‌های دیگر
  - بابک صاحب فایل B، اجازه نوشتن را به علی می دهد.
  - علی فایل A را می خواند و در فایل B می نویسد.
  - علی دیگر هیچ کنترلی روی B (حاوی اطلاعات A) ندارد.
- عدم امکان کنترل جریان اطلاعات از یک شیئ به شیئ دیگر
- با فرض معتمد بودن عامل‌ها
  - به نرم‌افزارها نمی‌توان اعتماد کرد.
  - احتمال وجود اسب تروا (Trojan Horse)



ضعف کنترل دسترسی اختیاری

- احتمال وجود اسب تروا (Trojan Horse)



کنترل دسترسی اجباری

- کنترل دسترسی عامل‌ها به اشیاء بر اساس سطوح امنیتی آنها و قواعد ثابت
- **مدل‌های حفظ محرمانگی** ← *تمرکز این درس*
  - مثال: مدل BLP
- مدل‌های حفظ صحت
  - مثال: مدل Biba
- مدل‌های حفظ صحت و محرمانگی
  - مثال: مدل Dion

مدل BLP

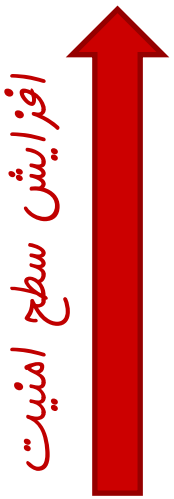
- ارائه شده به وسیلهٔ Bell و Lapadula در سال ۱۹۷۶
- توسعه‌یافتهٔ مدل ماتریس دسترسی برای حفظ امنیت چندسطحی
- مناسب برای محیط‌های نظامی
- عامل‌ها و اشیاء دارای سطح امنیتی (سطح محرمانگی)

مدل BLP

- دو نوع سطح امنیتی (سطح محرمانگی):
  - **سطح محرمانگی عامل:** میزان اعتماد به فرد (عامل) در عدم افشای داده‌های یک شیئ.
  - **سطح محرمانگی شیئ:** میزان محرمانگی داده‌های یک شیئ و میزان خسارت ناشی از افشای غیرمجاز داده‌های آن.

مدل BLP

- مثالی از سطوح رده‌بندی عامل‌ها (یا برنامه‌ها) و اشیاء (یا منابع):
  - خیلی سری یا TS (مخفف Top Secret)
  - سری یا S (مخفف Secret)
  - محرمانه یا C (مخفف Confidential)
  - بدون رده یا U (مخفف Unclassified)



- **رابطه تفوق (dominance):** برای مقایسه دو سطح امنیتی

$$L1 \geq L2$$

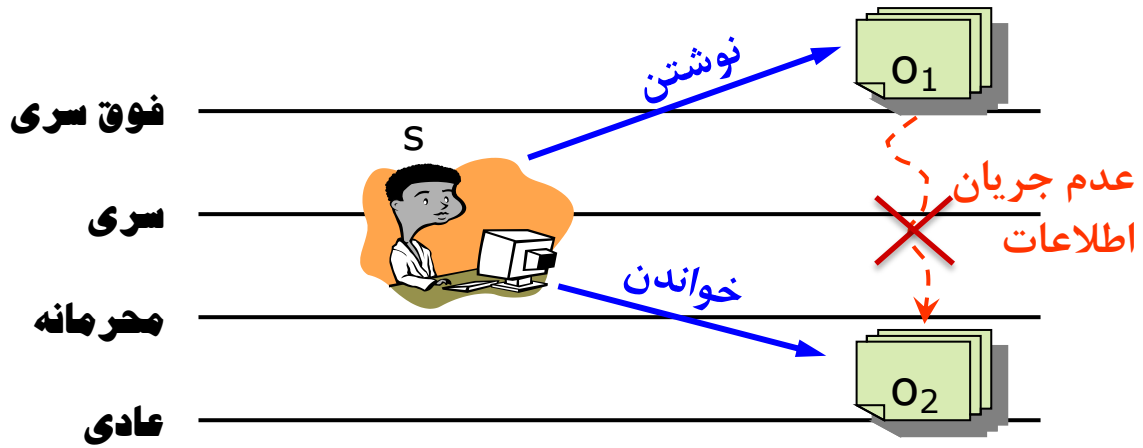
خلاصه اصول دسترسی BLP

۱ عامل‌ها می‌توانند از اشیای با سطوح امنیتی پایین‌تر یا مساوی خود، بخوانند.

No Read Up

۲ عامل‌ها می‌توانند در اشیای با سطوح امنیتی بالاتر یا مساوی خود، بنویسد.

No Write Down



فهرست مطالب

- مقدمه
- مدل‌های کنترل دسترسی اختیاری
- مدل‌های کنترل دسترسی اجباری
- **مدل‌های کنترل دسترسی نقش-مبنا**

مدل نقش–مبنا

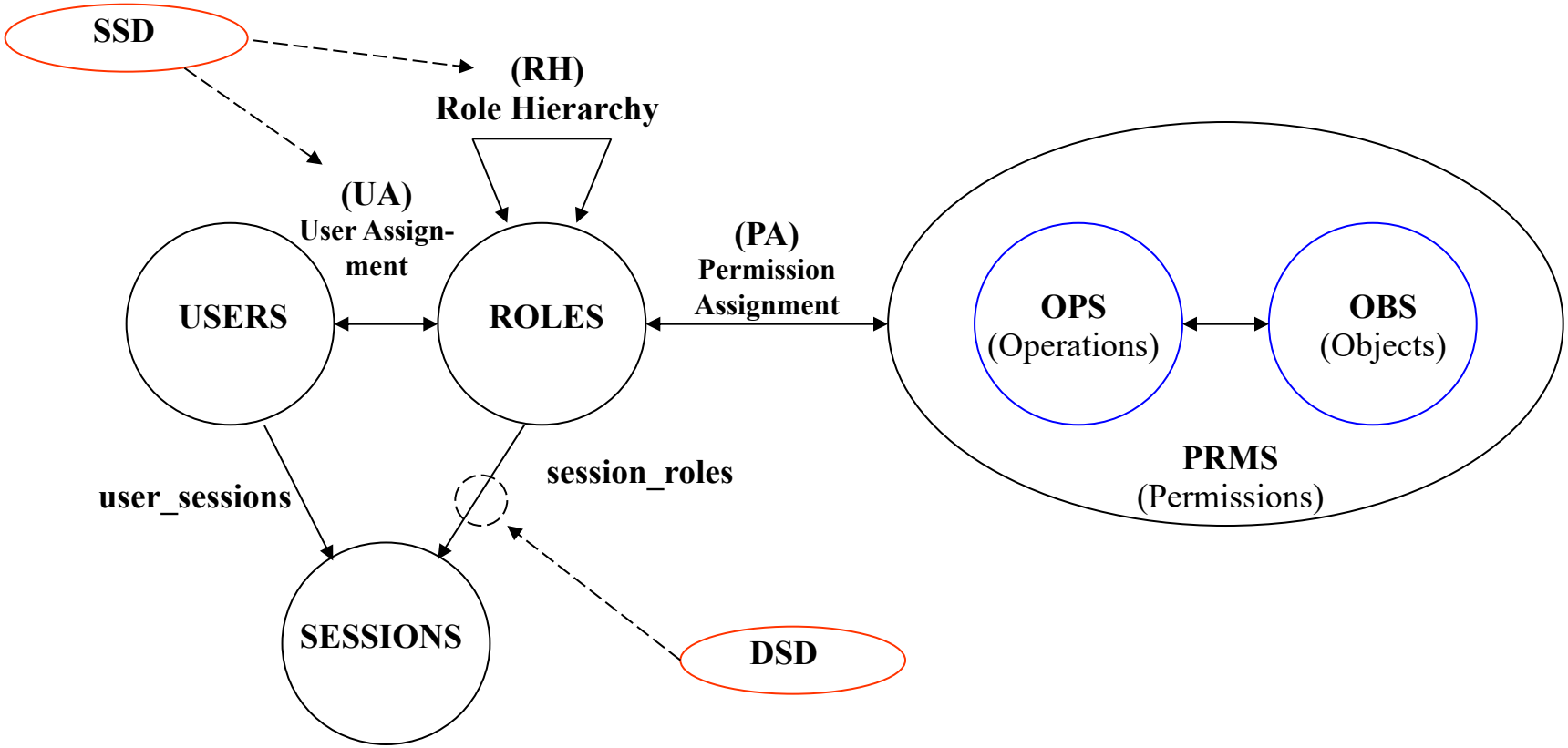
- اعطای مجوزها به نقش‌ها و نقش‌ها به کاربران (به جای اختصاص مستقیم مجوزها به کاربران)
- اعطای مجموعه مجوزهای موردنیاز به هر نقش برای اجرای وظایف محوله
- اعطا و فعال‌سازی نقش‌ها بر اساس اصل حداقل مجوزها
- امکان اِعمال محدودیت‌های
  - تفکیک وظایف (Separation of Duties)
  - مساله تضاد منافع (Conflict of Interests)

مدل نقش–مبنا (RBAC)

- خصوصیات اصلی مدل نقش-مبنای RBAC:
  - سازگاری با ساختار سازمانی
  - سادگی مدیریت کنترل دسترسی
  - اصل حداقل مجوزها (Least Privilege)
  - امکان اعمال محدودیت‌های تفکیک وظایف (SoD) و تضاد منافع

مدل RBAC

نمای کلی مدل



انواع مدل نقش–مبنا

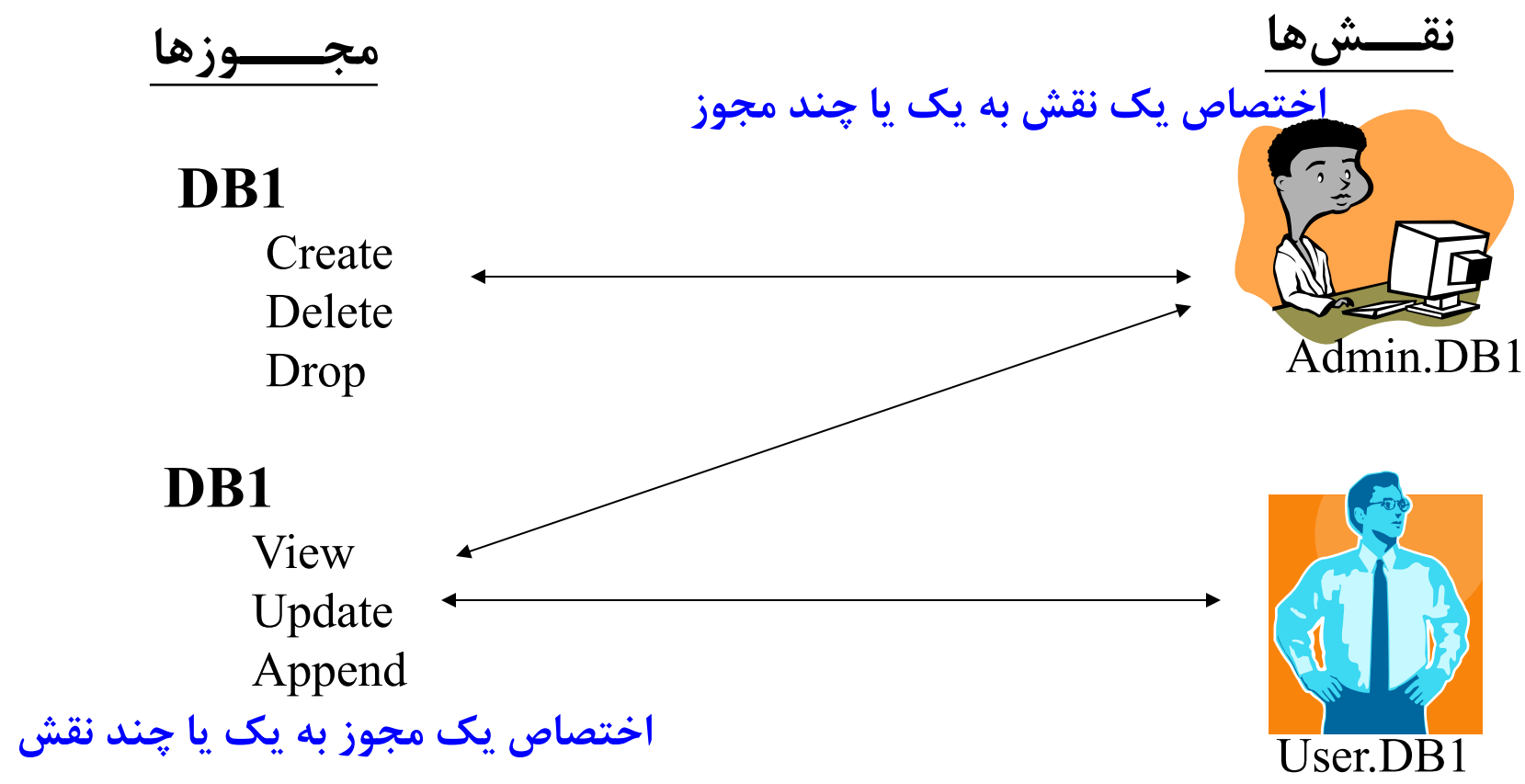
مدل	سلسله مراتب نقش‌ها	محدودیت تفکیک وظایف
$RBAC_0$	–	–
$RBAC_1$	✓	–
$RBAC_2$	–	✓
$RBAC_3$	✓	✓

مدل نقش مبنای پایه $RBAC_0$

- مولفه‌های مدل پایه $RBAC_0$:
  - عامل‌ها یا کاربران(USERS)
  - نقش‌ها (ROLES)
  - مجوزها (PRMS)
    - اعمال (OPS)
    - اشیاء (OBS)
  - رابطه اختصاص نقش به کاربر (UA)
  - رابطه اختصاص مجوز به نقش (PA)
  - نشست‌ها (SESSIONS)

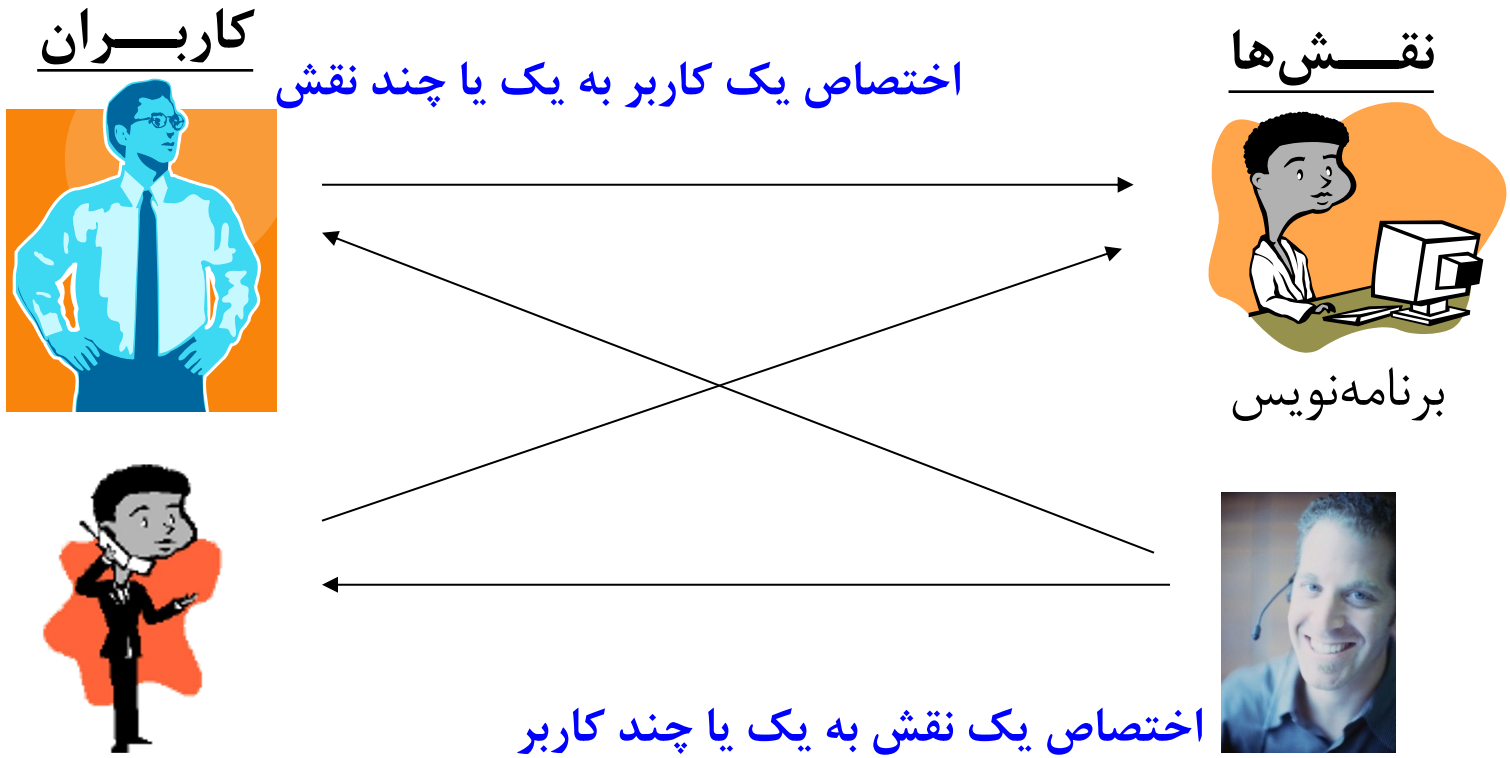
مدل $RBAC_0$

- رابطه اختصاص مجوز به نقش (PA)



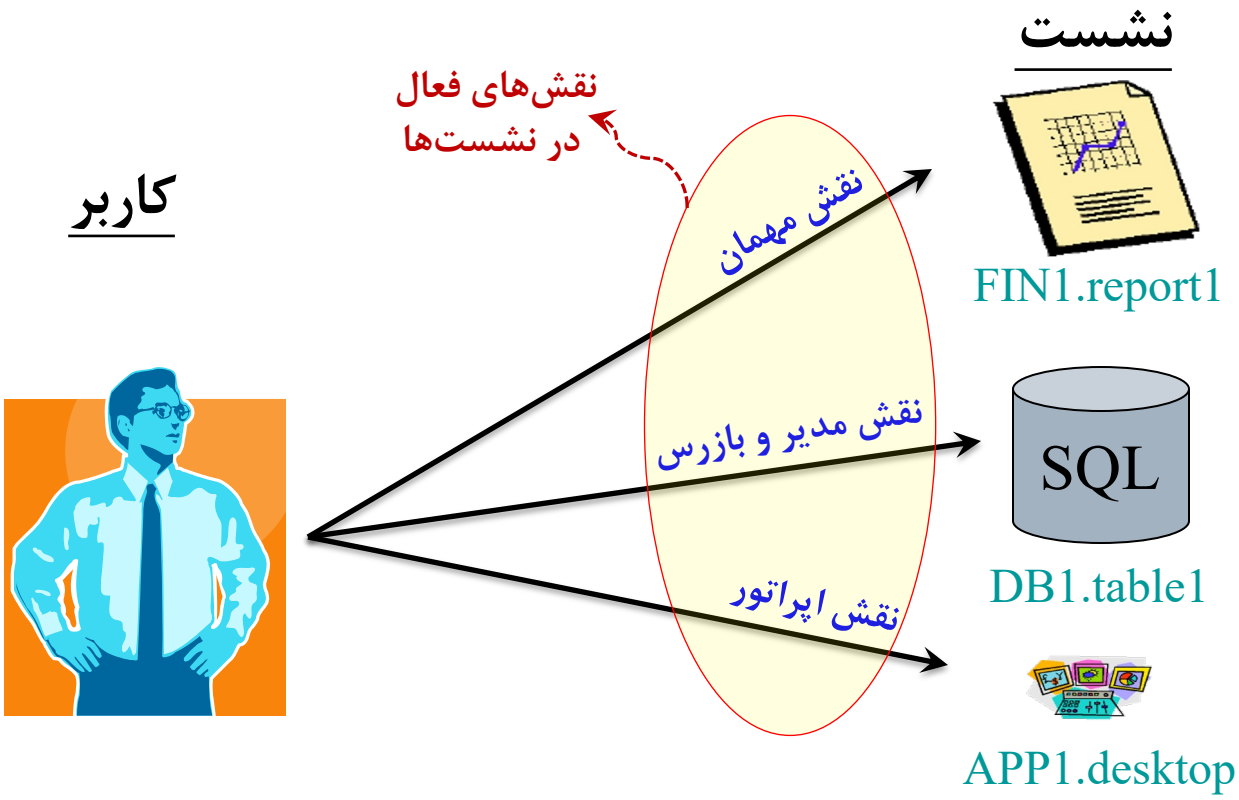
مدل $RBAC_0$

- رابطه اختصاص نقش به کاربر (UA)



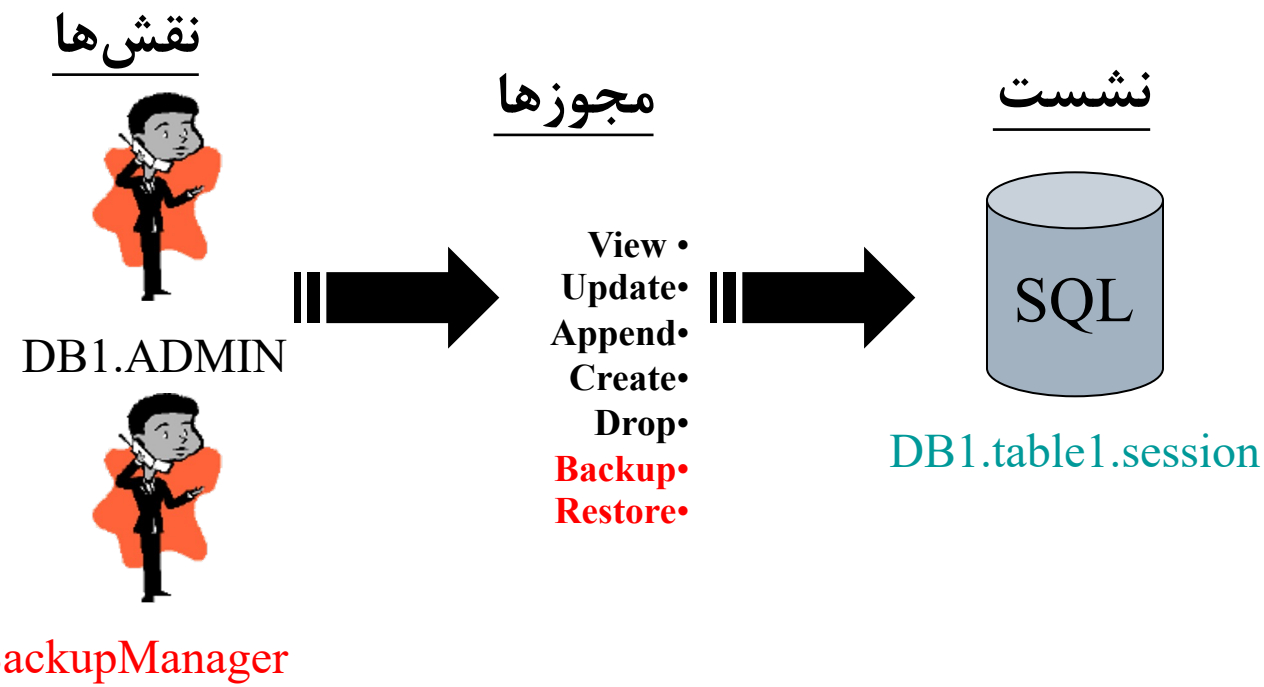
مدل $RBAC_0$

- **نشست‌ها:** هر کاربر می تواند چند نشست داشته باشد و در هر نشست می‌تواند زیرمجموعه‌ای از نقشهای اختصاص یافته را فعال کند.



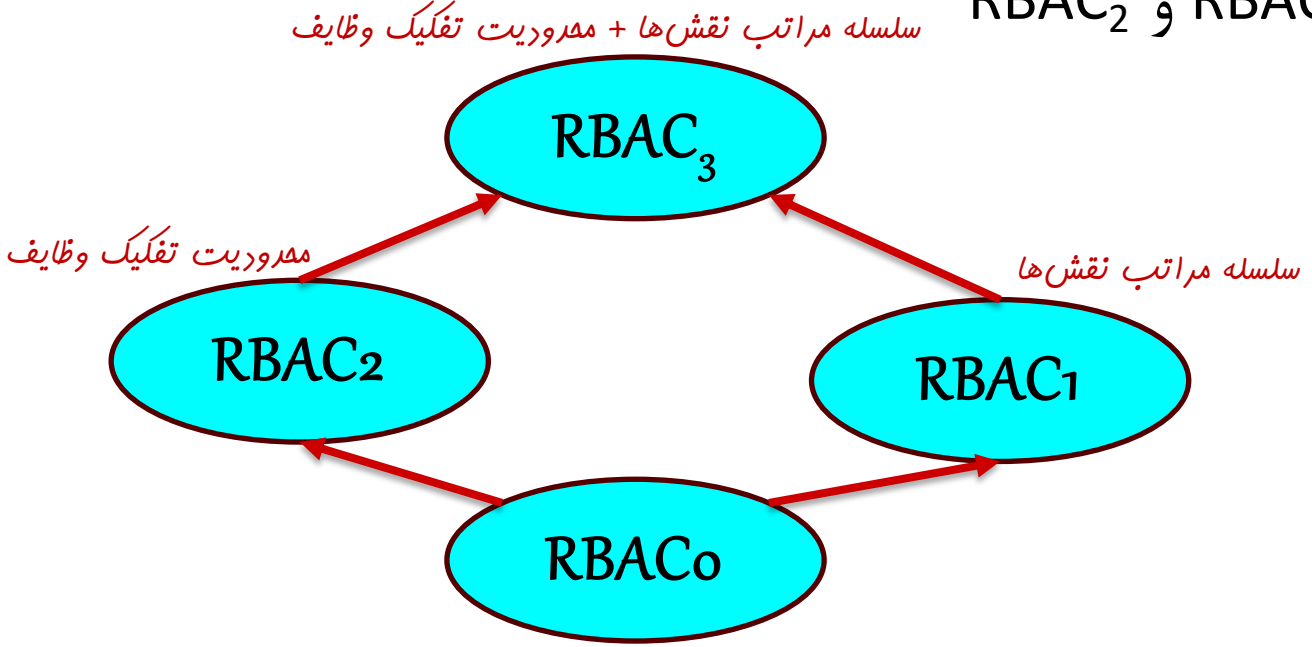
مدل $RBAC_0$

- مجوزهای یک نشست = مجموعه مجوزهای نقش‌های فعال شده در نشست



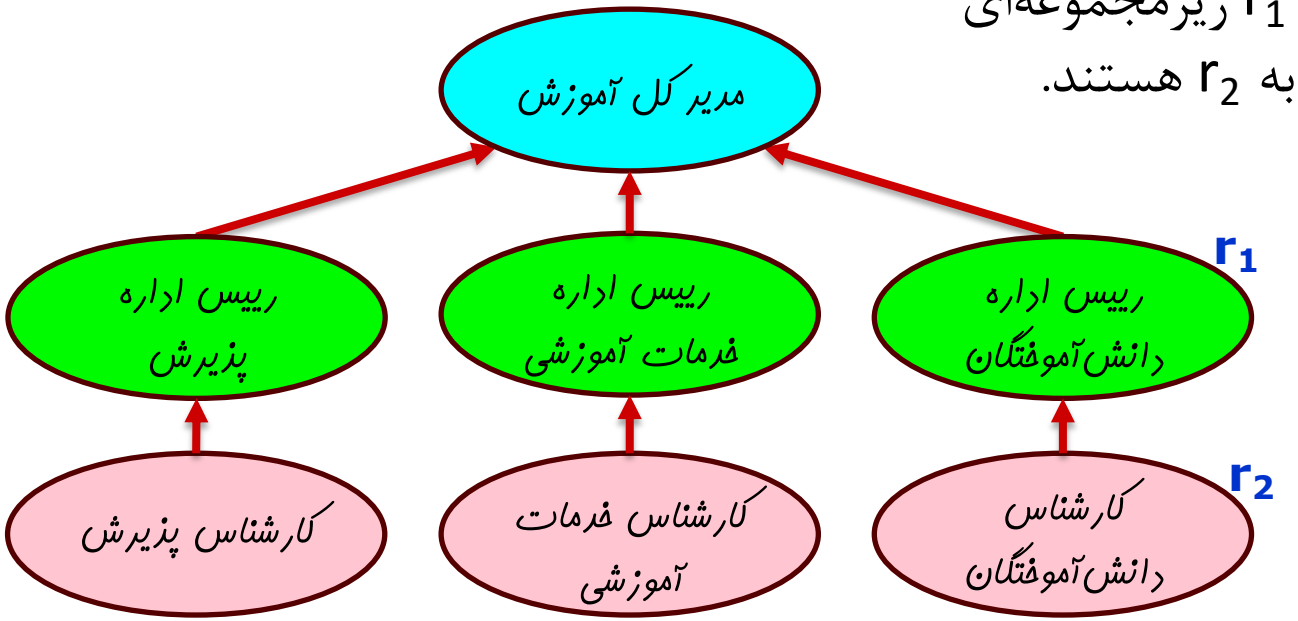
انواع دیگر مدل RBAC

- به کارگیری مفهوم سلسله مراتب نقش‌ها منطبق بر ساختار سازمانی در $RBAC_1$
- محدودیت‌های تفکیک وظایف (SoD) در $RBAC_2$ برای جلوگیری از سوءاستفاده از اختیارات توسط افراد
- $RBAC_3$ ترکیبی از $RBAC_1$ و $RBAC_2$



مدل $RBAC_1$ – سلسله مراتب نقش‌ها

- یک سلسله مراتب از نقش‌ها بر اساس رابطه زیرنقش بودن (مطابق با ساختار سازمانی)
- اگر r_2 زیرنقش r_1 باشد ($r_1 \geq r_2$):
  - r_1 تمام مجوزهای r_2 را به ارث می‌برد.
  - کاربران منتسب به r_1 زیرمجموعه‌ای از کاربران منتسب به r_2 هستند.



مدل $RBAC_2$ – محدودیت تفکیک وظایف

- **محدودیت تفکیک وظایف (SoD- Separation of Duty):**
  یک کاربر نمی‌تواند چند نقش مشخص را توأمان داشته باشد.

- **مثال:** در بانک، یک کاربر نمی‌تواند هم نقش صادرکننده چک و هم نقش امضاکننده چک را داشته باشد.

- تفکیک وظایف مانع از سوءاستفاده در سازمان به دلیل اعطای اختیارات (مجوزهای) بیش از حد به یک فرد می‌شود.

- **توجه:** البته همچنان با تبانی کاربران چند نقش، امکان سوءاستفاده وجود دارد.

توصیف دقیقتر انواع مدل‌های کنترل دسترسی در درس امنیت پایگاه داده‌ها

پایان

پست الکترونیکی

amini@sharif.edu

kharrazi@sharif.edu