به نام خدا

اسماعیل زارع

کنترل دسترسی اختیاری(DAC) چیست؟

کنترل دسترسی اختیاری یک مدل کنترل دسترسی مبتنی بر هویت است که میزان مشخصی از کنترل بر روی داده‌های خود را در اختیار کاربران قرار می‌دهد .صاحبان داده ها (سازندگان اسناد یا هر کاربر مجاز به کنترل داده ها) می توانند مجوزهای دسترسی را برای کاربران یا گروه هایی از کاربران خاص تعریف کنند .به عبارت دیگر، با صلاحدید مالک منبع، به چه کسی دسترسی داده شود و چه امتیازاتی اعطا شود.

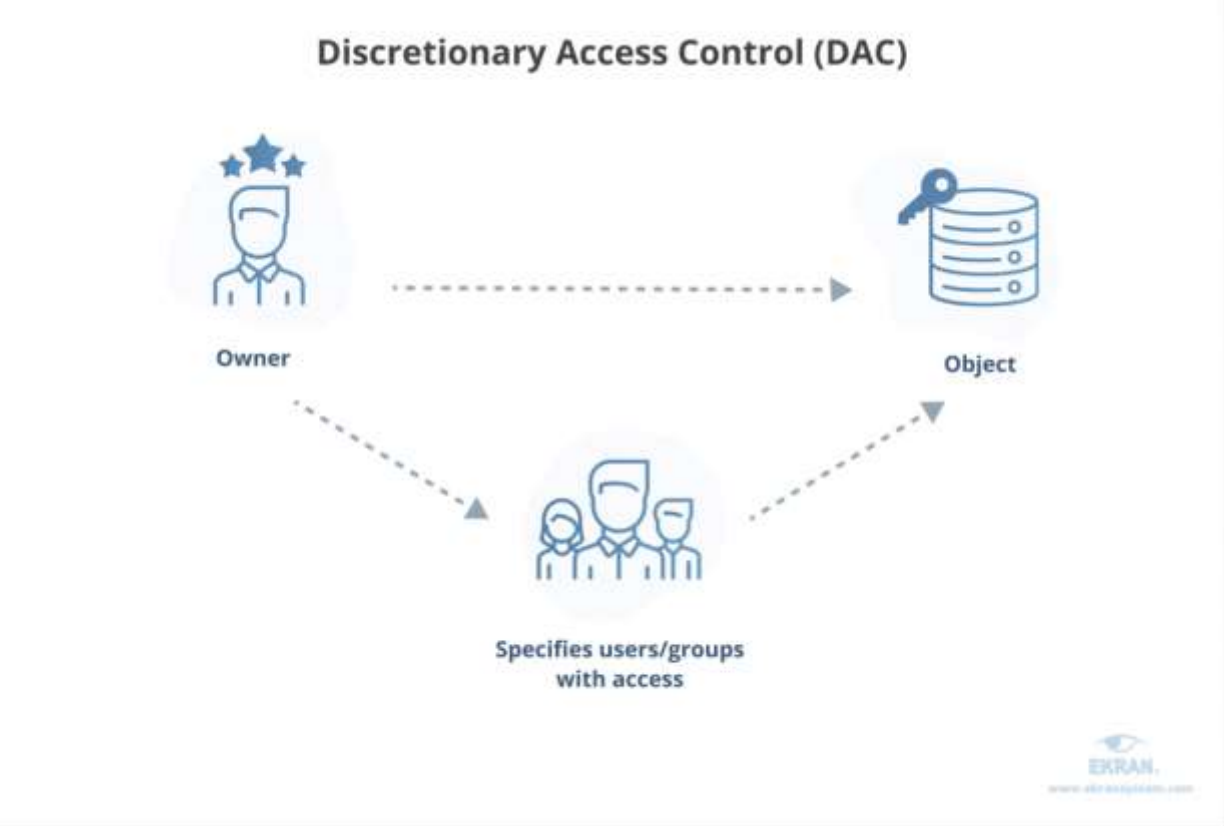
مجوزهای دسترسی برای هر قطعه داده در یک لیست کنترل دسترسی (ACL) ذخیره می شود .زمانی که کاربر به شخصی اجازه دسترسی می دهد، یک مدیر این لیست را ایجاد می کند .لیست را می توان به طور خودکار تولید کرد . ACLشامل کاربران و گروه هایی است که ممکن است به داده ها و سطوح دسترسی آنها دسترسی داشته باشند .یک مدیر سیستم همچنین می تواند ACL را اعمال کند .در این مورد، ACLبه عنوان یک سیاست امنیتی عمل می کند و کاربران عادی نمی توانند آن را ویرایش یا لغو کنند.

اصول اولیه DAC چیست؟

۱- ویژگی های شی (اندازه، نام، مسیر دایرکتوری) برای کاربرانی که مجاز نیستند نامرئی هستند.

۲- چندین تلاش برای دسترسی ناموفق، احراز هویت چند عاملی اضافی را اعمال می‌کنند یا دسترسی را رد می‌کنند.

۳- کاربران می توانند مالکیت شی خود را به سایر کاربران منتقل کنند .همچنین مالک نوع دسترسی سایر کاربران را تعیین می کند .بر اساس این امتیازات دسترسی، سیستم عامل تصمیم می گیرد که آیا اجازه دسترسی به یک فایل را بدهد یا خیر.



دسترسی به یک فایل در مدل DAC به صورت زیر عمل می کند:

- کاربر ۱ یک فایل ایجاد می کند و مالک آن می شود یا حقوق دسترسی به یک فایل موجود را به دست می آورد.
- کاربر ۲ درخواست دسترسی به این فایل را دارد .آنها اعتبار خود را ارائه می دهند: نام کاربری، رمز عبور یا چیز دیگری.
- کاربر ۱ به صلاحدید خود اجازه دسترسی می دهد .با این حال، کاربر ۱ نمی تواند حقوق دسترسی بیش از حقوق خود را اعطا کند .برای مثال، اگر کاربر ۱ فقط بتواند یک سند را بخواند، نمی تواند به کاربر ۲ اجازه دهد آن را ویرایش کند.
- اگر هیچ تناقضی بین ACL ایجاد شده توسط مدیر و تصمیم اتخاذ شده توسط کاربر ۱ وجود نداشته باشد، دسترسی داده می شود.

کنترل دسترسی اختیاری یک مدل کاملاً محبوب است زیرا آزادی زیادی را برای کاربران فراهم می کند و باعث سربار اداری نمی شود .با این حال، چندین محدودیت قابل توجه دارد.

مزایا و معایبDAC

طرفداران

- **کاربر پسند** -کاربران می توانند داده های خود را مدیریت کنند و به سرعت به داده های سایر کاربران دسترسی داشته باشند.
- **انعطاف پذیر** -کاربران می توانند پارامترهای دسترسی به داده را بدون سرپرست پیکربندی کنند.
- **نگهداری آسان** —افزودن اشیاء و کاربران جدید زمان زیادی را برای مدیر نمی گیرد.
- **دانه بندی** -کاربران می توانند پارامترهای دسترسی را برای هر قطعه داده پیکربندی کنند.

منفی

- **سطح پایین حفاظت از داده** DAC -نمی تواند امنیت قابل اعتمادی را تضمین کند زیرا کاربران می توانند داده های خود را هر طور که دوست دارند به اشتراک بگذارند.
- **مدیریت دسترسی مبهم** -هیچ مدیریت دسترسی متمرکز وجود ندارد، بنابراین برای یافتن پارامترهای دسترسی، باید هر ACL را بررسی کنید .
- **همپوشانی امتیازات کاربر** -ممکن است تضاد مجوزها با کاربران چندین گروه کاری تودرتو رخ دهد .

DAC نباید توسط سازمان هایی که با داده های بسیار حساس (پزشکی، مالی، نظامی و غیره) کار می کنند به چند دلیل استفاده شود:

- اگر کاربر ۱ حقوق دسترسی را با کاربر ۲ به اشتراک بگذارد، هیچ تضمینی وجود ندارد که کاربر ۲ برای کار کردن به این دسترسی نیاز داشته باشد، داده ها را سرقت یا خراب نکند و به یک کاربر مخرب دسترسی ندهد.
- کنترل جریان اطلاعات در داخل شبکه غیرممکن است.
- اجرای اصول کمترین امتیاز، نیاز به دانستن و تفکیک وظایف غیرممکن است.

مدل کنترل دسترسی اختیاری یا DAC کمترین محدودیت را در مقایسه با محدودترین مدل MAC دارد. DAC به یک فرد اجازه می دهد تا کنترل کاملی بر هر شیئی که در اختیار دارد همراه با برنامه های مرتبط با آن اشیاء داشته باشد.

این به DAC دو ضعف عمده می دهد:

اول، به کاربر نهایی کنترل کامل می‌دهد تا تنظیمات سطح امنیتی را برای سایر کاربران تنظیم کند که می‌تواند باعث شود کاربران از امتیازات بالاتری نسبت به آنچه که قرار است برخوردار شوند.

ثانیا، و بدتر از آن، مجوزهایی که کاربر نهایی دارد به برنامه های دیگری که آنها اجرا می کنند به ارث می رسد. این بدان معناست که کاربر نهایی می‌تواند بدافزار را بدون اطلاع از آن اجرا کند و بدافزار می‌تواند از امتیازات بالقوه سطح بالایی که کاربر نهایی دارد استفاده کند.

در عین حال، DACانتخاب خوبی برای مشاغل کوچک با کارکنان محدود فناوری اطلاعات و بودجه امنیت سایبری است .این امکان به اشتراک گذاری اطلاعات را فراهم می کند و عملکرد روان کسب و کار را تضمین می کند .این رویکرد، زمانی که در سازمانی با ۱۰ تا ۲۰ کارمند اعمال می شود، فاقد پیچیدگی و چالش های نظارتی مرتبط با استفاده از DACدر سازمان هایی با صدها یا هزاران کارمند است.