March 11, 2020

Mandatory Access Control vs Discretionary Access Control: Which to Choose?

Category: Security

Access control is one of the most important cybersecurity practices. Careful adjustment of users' access rights helps to secure sensitive data and reduces the chance of a successful attack.

However, choosing a relevant access control model can be tricky. In one of our previous posts, we reviewed role-based and attribute-based access control models. In this post, we discuss definitions of, implementations of, and use cases for the mandatory and discretionary access control models. We also compare two approaches to choosing one over the other.

Why is access control important?

Access control regulates which users, applications, and devices can view, edit, add, and delete resources in an organization's environment. Controlling access is one of the key practices to protect sensitive data from theft, misuse, abuse, and any other threats. There are two levels of access control: physical and logical.

Access control helps to mitigate both insider and outsider threats. That's why IT regulations and standards — NIST, HIPAA, PCI DSS, and others — enforce strict physical and logical access control measures. In this article, we discuss models of logical access control.

There are several logical access control models: mandatory, discretionary, role-based, attribute-based, etc. The process of choosing and deploying an access control model looks different for each organization. This choice depends on:

- The nature of the protected data
- IT requirements and industry standards
- The number of employees
- The cybersecurity budget

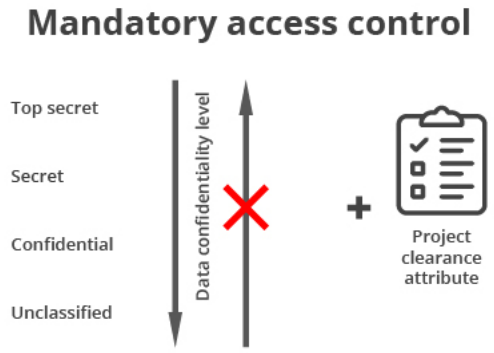
Let's find out when to use mandatory and discretionary access control models.

Read also:
Role-based Access Control vs Attribute-based Access Control: How to Choose

What is mandatory access control?

Mandatory access control (MAC) is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on a **need to know** basis: users have to prove a need for information before gaining access.

MAC is considered the most secure of all access control models. Access rules are manually defined by system administrators and strictly enforced by the operating system or security kernel. Regular users can't alter security attributes even for data they've created.



With MAC, the process of gaining access looks like this:

- The administrator configures access policies and defines security attributes: confidentiality levels, clearances for accessing different projects and types of resources.
- The administrator assigns each subject (user or resource that accesses data) and object (file, database, port, etc.) a set of attributes.
- When a subject attempts to access an object, the operating system examines the subject's security attributes and decides whether access can be granted.

For example, let's consider data that has the "top secret" confidentiality level and "engineering project" security label. It's available to a set of users that have "top secret" clearance and authorization to access engineering documents. Such users can also access information that requires a lower level of clearance. But employees with lower levels of clearance will not have access to information that requires a higher level of clearance

MAC brings lots of benefits to a cybersecurity system. But it has several disadvantages to consider.

Pros and cons of MAC

Pros

High level of data protection — An administrator defines access to objects, and users can't edit that access.
Granular — An administrator sets user access rights and object access parameters manually.
Immune to Trojan Horse attacks — Users can't declassify data or share access to classified data.

Cons

Maintainability — Manual configuration of security levels and clearances requires constant attention from administrators.
Scalability — MAC doesn't scale automatically.
Not user-friendly — Users have to request access to each new piece of data; they can't configure access parameters for their own data.

When to use MAC

MAC is used by the **US government to secure classified information** and to support **multilevel security** policies and applications. This access control model is mostly used by government organizations, militaries, and law enforcement institutions. It's reasonable to use MAC in organizations that value data security more than operational flexibility and costs. Implementing MAC in a private organization is rare because of the complexity and inflexibility of such a system.

A pure MAC model provides a high and granular level of security. On the other hand, it's difficult to set up and maintain. That's why it's common to combine MAC with other access control models.

For example, combining it with the role-based model speeds up the configuration of user profiles. Instead of defining access rights for each user, an administrator can create user roles. Each organization has users with similar roles and access rights: employees with the same job position, third-party vendors, etc. An administrator can configure roles for these groups instead of configuring individual user profiles from scratch.

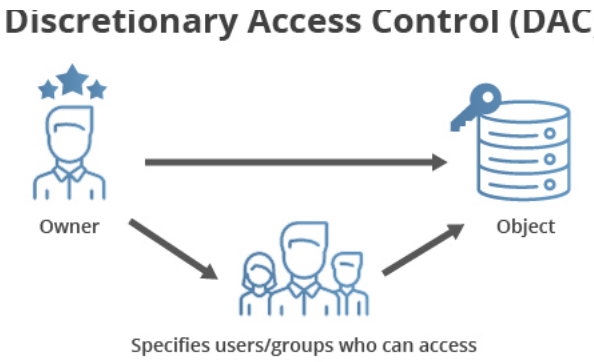
Another popular combination is MAC and the discretionary access control (DAC) model. MAC can be used to secure sensitive data, while DAC allows coworkers to share information within a corporate file system.

Read also:
Key Features of an Insider Threat Protection Program for the Military

What is discretionary access control?

Discretionary access control (DAC) is an **identity-based access control model** that provides users a certain amount of control over their data. Data owners (or any users authorized to control data) can define access permissions for specific users or groups of users.

Access permissions for each piece of data are stored in an **access-control list** (ACL). This list can be generated automatically when a user grants access to somebody or can be created by an administrator. An ACL includes users and groups that might access data and levels of access they might have. An ACL can also be enforced by a system administrator. In this case, the ACL acts as a security policy, and regular users can't edit or overrule it.



Gaining access in the DAC model works like this:

User 1 creates a file and becomes its owner or obtains access rights to an existing file.
User 2 requests access to this file.
User 1 grants access at their own discretion. However, user 1 can't grant access rights that exceed their own. For example, if user 1 can only read a document, they can't allow user 2 to edit it.
If there's no contradiction between the ACL created by an administrator and the decision made by user 1, access is granted.

Discretionary access control is quite a popular model because it allows a lot of freedom for users and doesn't cause administrative overhead. However, it has several considerable limitations.

Pros and cons of DAC

Pros

User-friendly — Users can manage their data and quickly access data of other users.
Flexible — Users can configure data access parameters without administrators.
Easy to maintain — Adding new objects and users doesn't take much time for the administrator.
Granular — Users can configure access parameters for each piece of data.

Cons

Low level of data protection — DAC can't ensure reliable security because users can share their data however they like.
Obscure — There's no centralized access management, so in order to find out access parameters, you have to check each ACL.

When to use DAC

DAC allows for a lot of flexibility and decreases the load on system administrators as users can manage access on their own. On the other hand, it doesn't provide a high level of security for several reasons:

If user 1 shares access rights with user 2, there's no guarantee that user 2 needs this access to work or won't steal or corrupt data or grant access to a malicious user.
It's impossible to control information flows inside the network.

Contact us

Because of these limitations, DAC can't be used by organizations that work with extremely sensitive data (medical, financial, military, etc.).

At the same time, DAC is a good choice for small businesses with limited IT staff and cybersecurity budgets. It allows for sharing information and ensures the smooth operation of the business. This approach, when applied in an organization with 10 to 20 employees, lacks the complexity and oversight challenges associated with the use of DAC in organizations with hundreds or thousands of employees.

Comparing the two approaches

Let's review the key characteristics of these two access control models:

Characteristic	MAC	DAC
Access control enforced by	Administrators and operating system	Administrators and users
Flexibility	–	✓
Scalability	–	✓
Simplicity	–	✓
Maintenance	Hard	Easy
Implementation cost	High	Low
Granularity	High (admins adjust clearances for each user and object manually)	High (users can assign access rights for any other user or group)
Easy to use	–	✓
Security level	High	Low
Useful for	Government, military, law enforcement	Small and medium-sized companies

MAC and DAC are very different access control models, suitable for different kinds of organizations. DAC works well for organizations that require flexibility and user-friendly workflows. On the other hand, MAC is more efficient for organizations that work with highly sensitive data.

Conclusion

MAC and DAC are two opposite models of access control. MAC is controlled by administrators and requires lots of time and effort to maintain, but it provides a high level of security. DAC is much easier to implement and maintain, as users can manage access to the data they own. However, DAC isn't good enough for protecting sensitive data.

With Ekran System, you can implement either of these access control models. The Ekran platform has **Privileged Access Management** functionality that allows you to enforce access policies of any complexity. With just-in-time PAM methods from Ekran System, you can also control user access manually by making users request access to the most critical resources and providing one-time passwords instead of granting privileges.

environments.

Additionally, Ekran can enforce a role-based access control model. This model is considered to strike a good balance between security and manageability.

Learn more about role-based access control.

YOU MAY ALSO LIKE

Key Features of an Insider Threat Protection Program for the Military

January 30, 2020

Insider threat protection is an essential activity for government institutions — and especially for national defense organizations. Although cybersecurity in...

Ekran System Inc. Moves to Newport Beach, CA

January 17, 2020

Ekran System Inc. is pleased to announce the opening of our new US headquarters. We're saying goodbye to our long-time headquarters in San Antonio, Texas, and...

Secrets Management: Importance, Challenges, Best Practices

November 26, 2019

To ensure proper protection of their critical data, organizations pay attention to the processes they use for managing identities, privileges, and secrets....

Insider Threats in the US Federa Government: Detection and Prevention

October 04, 2019

Governments are one of the biggest cybersecurity spenders. In 2015, for example, the US government include billion in cybersecurity spending in t

TRY IT NOW

Get started today by deploying a trial version in your company or try a free demo online

DOWNLOAD TRIAL VERSION

TRY ONLINE

SUBSCRIBE TO UPDATES

Your email

SUBSCRIBE

Resources

Partners

Company

Support

Blog

Buy

Contact us

Privacy Policy EULA
260 Newport Center Drive Suite 425, Newport Beach, California 92660, USA
D-U-N-S number: 089270023
CAGE number: 88VL6

Contact us