Access Control Models Cheat Sheet

by xoulea via cheatography.com/198356/cs/43340/

INTRODUCTION

Access control is an essential aspect of information security that regulates access to resources based on predefined policies. Access control models determine the permissions granted to users or processes and the level of access they have to different resources. Several access control models have been developed to address different security requirements, such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), Context-Based Access Control (CBAC), and Risk-Adaptive Access Control (RAC)..

ACCESS CONTROL MODELS

RBAC	RBAC is an access control model that associates permissions with roles rather than individual users. This model provides a scalable and flexible approach to access control, enabling the management of large and complex systems. RBAC assigns users to roles based on their job functions and responsibilities and allows administrators to manage permissions at the role level. Users can perform their tasks and access resources based on the permissions associated with their roles. This model is widely used in organizations, such as healthcare, finance, and government, to control access to sensitive data and resources.
ABAC	ABAC is an access control model that uses attributes to determine access to resources. This model enables a fine-grained and context-aware approach to access control, where access decisions are based on user attributes, resource attributes, environmental attributes, and policy attributes. ABAC policies can be expressed in a formal language, such as XACML, and can be evaluated dynamically at runtime. This model is suitable for complex and dynamic environments, such as cloud computing and IoT, where access decisions are based on various factors, such as location, time, and device.
MAC	MAC is an access control model that enforces a hierarchical and rigid access control policy. In MAC, the access rights to resources are determined by the system administrator or security policy, and users have limited control over their permissions. This model is commonly used in government and military environments to protect classified information and ensure data confidentiality. MAC provides a high level of security but can be challenging to manage and administer.
DAC	DAC is an access control model that grants users full control over their resources, enabling them to set permissions and share resources with other users. This model is widely used in personal computing and small-scale systems, where users need flexibility and control over their resources. DAC provides a simple and intuitive approach to access control but can be challenging to scale and manage in large and complex systems.
CBAC	CBAC is an access control model that uses contextual information to determine access to resources. This model considers various factors, such as user identity, device location, time of day, and network topology, to make access decisions. CBAC provides a dynamic and adaptable approach to access control, enabling organizations to respond quickly to changing security threats and environmental factors. CBAC is suitable for environments, such as healthcare and finance, where access decisions are based on multiple factors.

ACCESS CONTROL MODELS (cont)

RAC	RAC is an access control model that uses risk assessments to determine access to resources. This model evaluates various factors, such as user behavior, resource sensitivity, and environmental conditions, to calculate the level of risk associated with a particular access request. RAC policies can be dynamically adjusted based on the level of risk and can enable organizations to balance security and usability. RAC is suitable for environments, such as e-commerce and online banking, where access decisions are based on the level of risk associated with the transaction.