User Access Control Levels

Redback Operations

The document delves into the intricate realm of access control methodologies, dissecting the nuances between discretionary and non-discretionary access control mechanisms. In the former, users wield autonomy over resource access, while the latter places authority firmly in the hands of a centralized figure, typically an administrator.

Further exploration unfolds into the triad of access control paradigms: MAC, RBAC, and Temporal Access Control. MAC, reminiscent of military-grade security, rigidly imposes access parameters predefined by a central authority. RBAC, on the other hand, adopts a more flexible approach by assigning permissions based on predefined user roles, fostering scalability and manageability. Meanwhile, Temporal Access Control introduces the element of time, confining access within specified temporal boundaries, such as work hours.

The narrative navigates towards a preference for Dynamically Constrained Hierarchical RBAC (DCH-RBAC), extolling its added layer of control through the imposition of temporary constraints on existing roles. This augmented model promises finer-grained access control, elevating the efficacy of permission management. Hu (2006, et al) defines a Dynamically constrained system in NIST IR 7316 as a system where the abstract of access control is achieved via regulation of user’s actions using the definition of roles, role hierarchies, relationships, and constraints. This simplifies administration actions to granting and revoking roles based on the user’s role within the business and their needs.

However, the discourse doesn't shy away from confronting potential pitfalls inherent in RBAC and DCH-RBAC. Privilege escalation looms as a pertinent concern, wherein users with lower privileges might clandestinely ascend to higher echelons of access. Additionally, the labyrinthine nature of complex role structures can sow seeds of confusion regarding access entitlements.

Mitigation strategies emerge as beacons of hope amidst these challenges. The principle of least privilege advocates for the parsimonious allocation of access rights, limiting users to only what is essential for their roles. Regular audits serve as a bulwark against stagnation and inaccuracies, ensuring that access permissions remain commensurate with organizational needs. Moreover, the tenet of separation of duties advocates for the distribution of high-level access tasks among multiple users, mitigating the risk of a single point of failure.

In sum, the document embarks on a quest to architect a robust, secure, and efficient access control ecosystem for organizational resources, leveraging a melange of access control methodologies, pre-emptive measures against vulnerabilities, and strategic interventions to fortify the fabric of digital security.

**Top of Form**

**User Access Level Matrix (DCH-RBAC)**

This matrix proposes a Dynamically Constrained Hierarchical RBAC model with roles tailored for the company:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Description** | **Base Permissions** | **Dynamic Constraints (Optional)** |
| **Business Chair & Unit Staff Team** | Oversees team(s) and their leaders. | \* View all team and project details.  \* Manage team leader access.  \* View all company reports. | \* Can temporarily elevate Team Leader permissions for specific tasks (e.g., grant temporary access to edit another team's project). |
| **Team Leader** | Manages a specific team and its projects. | \* Manage Sub-Team Leader and Team Member access.  \* View all team project details. |  |
| **Sub-Team Leader** | Manages a specific team and its projects. | \* Manage sub-team member access.  \* View all sub-team project details. | \* Can temporarily elevate Team permissions for specific tasks (e.g., grant temporary access to edit another team's project). |
| **Sub-Team** | Completes projects | \* Create, Edit, and Delete projects (own sub-team).  \* Upload and Download project files. |  |

**Notes:**

* This is a sample matrix, and specific permissions can be adjusted based on company needs.
* DCH-RBAC allows for dynamic constraints to be applied to roles. These constraints can be time-based, project-specific, providing granular access control.
* Roles inherit permissions from higher levels in the hierarchy (e.g., Sub-Team Leader inherits permissions from Sub-Team).

This user access level matrix, based on DCH-RBAC principles, offers a balance between flexibility and security for company resources.

**References**

Hu, V. , Ferraiolo, D. and Kuhn, D. (2006), Assessment of access control systems:, , National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.7316 (Accessed May 11, 2024)