Segurança de Sistemas e Informação

(SEGSI)
PL04

*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: DACLs

Microsoft Active Directory uses a specific model to grant permissions to objects. It is possible to state, to a certain extent, what actions can be done to certain objects by a set of users. In this exercise, we want to create a pseudo environment where the student can understand what kind of Special permissions can be created in such an environment.

1. In the previous exercise you set up an Active Directory Service, create example groups such as **Finance, Service Desk, HR, SysAdmin**
2. Grant permissions such that service desk personnel is able to reset Finance User's Account Passwords
3. Grant Permissions for the SysAdmin personnel to add people to the Domain Administrator's group
4. Grant permissions to the HR department to Write the Personal Information of each employee
5. SysAdmin Accounts are able to change group memberships
6. What limitations do you foresee in considering this approach at scale?
7. Since you are giving permissions to users, what additional security controls should you apply to secure (or at least track) malicious actors?
8. Imagine that you want the exclude one person from a group's permission, how do you proceed? (Regarding effective permissions)

Exercise 2: RBAC

The new Standard for Access management is the Role Based Access Control Model. This model's implementation focuses heavily on ”What can someone do to something”, for instance, A user can write secrets on a Kubernetes ArgoCD namespace. This feature is implemented on several solutions and helps delegate responsibilities to be more refined and apply the least privilege security principle

1. To test this approach the simple thing to use is to bring up a Kubernetes Cluster. Spin up a Minikube Instance. [1]

2. Create three users [2]

3. Create at least three namespaces and their respective applications, you can use the examples from the Kubernetes repository. [3]

4. Assign roles to each user to each namespace

5. One User Can change deployments in any namespace, but it shouldn't be a cluster administrator.

6. Compare this model (RBAC) to the previously mentioned DACL model. How do they differ and what are the strengths and drawbacks of each one?

References

[1] [Online]. Available: https://minikube.sigs.k8s.io/docs/start/

[2] Aug 2023. [Online]. Available: https://kubernetes.io/docs/reference/access-authn-authz/rbac/

[3] Kubernetes, "Kubernetes/examples: Kubernetes application example tutorials." [Online]. Available: https://github.com/kubernetes/examples