UNIVERSIDADE FEDERAL DE SÃO PAULO
INSTITUTO DE CIÊNCIA E TECNOLOGIA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Trabalho Teórico 01

Tipos de Controle de Acesso

Nomes: Flávia Yumi Ichikura **RA:** 111791
Willian Dihanster Gomes de Oliveira **RA:** 112269

SÃO JOSÉ DOS CAMPOS
2019

Introdução

A segurança é uma das grandes preocupações da vida real e é algo refletido também na computação. Um exemplo é a de garantir acesso de dados ou sistemas apenas por pessoas autorizadas, em que se baseiam os algoritmos de controle de acesso.

A tarefa destes algoritmos, é dado uma solicitação, decidir se determinado usuário pode acessar o dado requisitado ou não de acordo com alguma política.

Ainda hoje, propõe-se novos algoritmos ou também variações, como os que serão detalhados neste trabalho, como o *Attribute-based access control, Break-glass e o Access control based on the responsibility*. Na próxima seção serão detalhados as funcionalidades e exemplos destes algoritmo e na última seção, as conclusões.

Attribute-based Access Control

O *Atribute-based Acess Control* (ABAC) consiste na ideia de controlar o acesso baseado em três tipos de atributos diferentes: atributos de usuário, atributos associados com a aplicação/sistema que será acessado e as atuais condições de ambiente. [1]

Este modelo também é um dos mais flexíveis e poderosos controles de acesso, no entanto, é o mais complexo. Além disso, permite um controle de acesso refinado, que permite mais variáveis de entrada para uma decisão de controle. Sendo assim, qualquer atributo disponível no diretório pode ser usado sozinho ou em uma combinação com outro, a fim de definir o filtro correto para controlar o acesso a um recurso.

Um exemplo deste modelo, seria permitir que somente usuários que são tipo *empregado* e são de departamento *x*, tenham acesso ao sistema de *Payroll* e somente durante o horário que trabalha.

Na Figura 1, temos um diagrama do funcionamento desta técnica de controle de acesso, que exemplifica os atributos utilizados, que ajudarão na decisão da permissão de acesso.

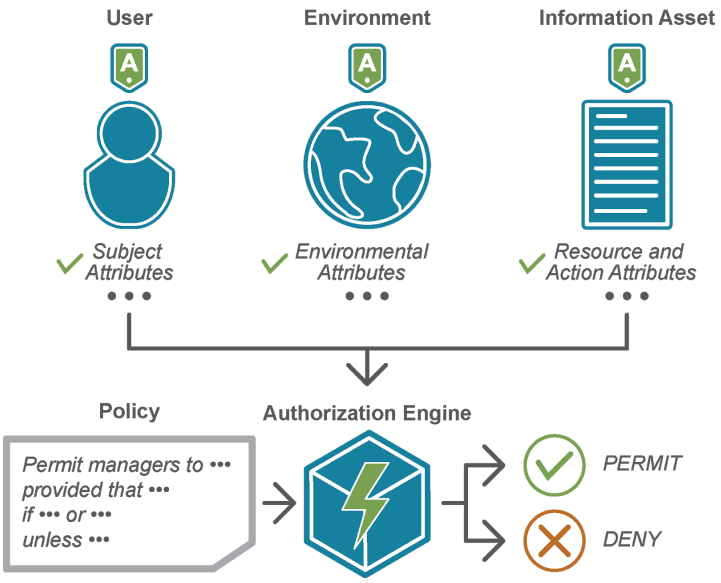

Figura 1: Diagrama de funcionamento do método de controle de acesso ABAC. Disponível em: https://www.axiomatics.com/attribute-based-access-control/

Break-glass

Como nem todos os casos de emergência e exceções são previsíveis, para que pessoas/atores não ficassem impedidas de realizarem suas tarefas, desenvolveu-se a abordagem *Break-glass*. *Break-glass* é uma política de segurança, baseada em liberar o acesso a algum recurso rapidamente a quem previamente não o possui, em casos no qual esse privilégio é necessário. [2]

Essa abordagem pode ser usada em sistemas que necessitam de login, como senha e usuário. Nela existem contas de emergência pré-definidas, gerenciadas de maneira a fazê-las disponíveis “passando por cima” da administração. [3]

As contas de emergência devem ser pré definidas, o usuário deve ser ter nome óbvio e significativo, porém as senhas devem difíceis. Os detalhes de como foram usadas, devem ser registrados para passar por auditoria. [3]

A política *Break-glass* pode ser utilizada em sistemas médicos, onde os dados dos pacientes devem estar disponíveis somente há uma parte do corpo de funcionários do hospital, fazendo uso então de contas para cada um deles. Há diversos casos, em que um funcionário pode não conseguir acessar sua conta, como quando esquece seu login e /ou senha, senha bloqueada por diversas tentativas falhas, erro no sistema, como quando ele está fora do ar. Em casos no qual o médico não consegue ter acesso aos dados do paciente, a saúde do paciente pode ser prejudicada devido ao tempo para conseguir resolver o problema. Se o sistema do hospital utilizar o *Break-glass*, o médico pode ter acesso facilmente a esses dados, diminuindo a probabilidade de ocorrerem danos. [3] Na Figura 2, temos um diagrama que exemplifica uma aplicação da técnica na área de hospitais, como fora explicado anteriormente. [3]

Figura 2: Exemplo de funcionamento do *Break-glass* na área hospital. Disponível em: https://www.semanticscholar.org/paper/Rumpole%3A-An-Introspective-Break-Glass-Access-Marinovic-Dulay/55175e22aaa1b19cd577ade3915b684ea8a724b7

Access control based on the responsibility

O método de *Access control based on the responsibility* ou ainda, ReMMo - *Responsibility MetaModel* partiu da ideia do RBAC - Role-Based Access Control.

RBAC é um método de controle de acesso baseado na função do usuário. Seu uso teve crescimento considerável em 2008, chamando atenção do pesquisador Christian Feltus. Fetus acabou listando problemas nesse método, como a análise insuficiente da função do usuário e a falta de alinhamento entre as responsabilidades dos usuários e os

acessos concedidos à eles. Assim propõe-se o ReMMo - *Responsibility MetaModel*, método de controle de acesso modelado a partir de três premissas: as obrigações do usuário, direitos para executar sua função e o processo de atribuir um usuário a uma responsabilidade. [4]

No método ReMMo, Fetus sugere que devem ser atribuídas responsabilidades aos usuários, e que as permissões de acesso devem estar atreladas às responsabilidades correspondentes.

Por exemplo, em uma empresa, há diversos estagiários, todos possuem o mesmo cargo na empresa, mas a cada um será dada uma responsabilidade diferente, dependendo por exemplo do setor que serão designados, desse modo a eles serão concedidos permissões a dados diferentes.

Conclusões

Sendo assim, conclui-se a importância das técnicas de controle de acesso na segurança de dados e sistemas computacionais. Além disso, como cada algoritmo possui sua particularidade, cada um possui suas vantagens, desvantagens e aplicações. O ABAC, por exemplo, pode ser indicado em sistemas que necessitem dar acesso a diferentes usuários, cada qual com seu acesso de acordo com um nível ou atributo chave, baseado em vários fatores/atributos como decisão. Já o *Break-glass,* é mais indicado em aplicações que possam haver situações de emergências e em que o acesso deva ser concedido, como um hospital. O ReMMo, pode ser indicado para situações onde os usuários necessitem e/ou trabalhem com o aspecto de responsabilidades.

Referências

[1] Carter, Samuel. “RBAC vs ABAC Access Control Models - IAM Explained”. Disponível em: https://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained. Acesso em 16/03/2019.

[2] Yale University. ”Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems”. Disponível em: https://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems. Acessado em 16/03/2019.

[3] Break-glass: An approach to granting emergency access to healthcare systems. White paper, Joint NEMA/COCIR/JIRA Security and Privacy Committee (2004).

[4] ELLIOT, Aaron; KNIGHT, Scott. A New Paradigm for Role-Based Access Control. Tese (Degree of Doctor of Philosophy) – Royal Military College of Canada / Collège militaire royal du Canada. 2018.