SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 04: MODELOS DE CONTROLES DE ACESSO

SUMÁRIO

Fatec Mauá

1. **Objetivo da Aula – Tópico da Ementa**
2. **Modelos de Controles de Acesso**
3. Modelo **Discricionário** (**DAC**)
4. Modelo **Obrigatório** (**MAC**)
5. Modelo **Baseado em Atributos** (**ABAC**)
6. Modelo **Baseado em Papéis** (**RBAC**)
7. Modelo **Baseado em Políticas** (**PBAC**)
8. Modelo de **Listas de Controle** (**ACL**)

1. OBJETIVO E EMENTA

Fatec Mauá

- **Objetivo da Aula**

  Proporcionar uma compreensão abrangente sobre os princípios de Controles de Acesso e Autorização, explorando as políticas de segurança, modelos e mecanismos de controle.

- **Tópico da Ementa**

  Conceitos fundamentais do pilar de segurança: confidencialidade, integridade, disponibilidade e autenticidade.

2. MODELOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

Fatec Mauá

➢ MODELOS de Controle de Acesso

- Os modelos de controle de acesso definem **como** os usuários podem **acessar** diferentes recursos em um sistema, como os **recursos** são **protegidos**. Eles são projetados para **limitar** o **acesso** a arquivos, dados e aplicações a **usuários autorizados**, quem tem **permissão** para acessá-los, prevenindo assim vazamentos de dados ou outras formas de comprometimento de segurança.

2. MODELOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

Fatec Mauá

➢ MODELOS de Controle de Acesso

- Os modelos de controle de acesso **estabelecem** o **framework** para:

  implementação de políticas de segurança

  mecanismos de controle

  administração de direitos de usuários e sistemas

2. MODELOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

Fatec Mauá

➢ MODELOS de Controle de Acesso

Existem vários modelos de controle de acesso:

- Controle de Acesso Discricionário (**DAC**)
- Controle de Acesso Obrigatório (**MAC**)
- Controle de Acesso Baseado em Atributos (**ABAC**)
- Controle de Acesso Baseado em Papéis (**RBAC**)
- Controle de Acesso Baseado em Políticas (**PBAC**)
- Listas de Controle de Acesso (**ACL**)

2. MODELOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

Fatec Mauá

➢ MODELOS de Controle de Acesso

- Cada modelo tem suas **vantagens**, **desvantagens** e **casos** de uso **ideais**.
- A escolha do modelo adequado depende dos **requisitos** específicos **de segurança**, da **natureza dos recursos** a serem protegidos, e da **estrutura organizacional**.
- Uma **combinação de modelos** pode ser utilizada para atender às necessidades de segurança de uma maneira abrangente e eficaz.

3. MODELO DISCRICIONÁRIO

Fatec Mauá

➢ Controle de Acesso Discricionário (**DAC**)

- **D**iscretionary **A**ccess **C**ontrol (**DAC**)
  No **DAC**, o controle de acesso é **baseado** na identidade do usuário e/ou nas **regras definidas** pelo **proprietário** do recurso: arquivo, diretório ou dispositivo. O proprietário determina **quem pode** acessar o recurso e **quais operações** podem ser realizadas. Este modelo é **flexível**, mas pode ser **menos seguro**, pois depende da discrição do proprietário, podendo conceder ou revogar permissões a outros usuários conforme desejar.

3. MODELO DISCRICIONÁRIO

Fatec Mauá

- Controle de Acesso Discricionário (**DAC**)

- **Vantagens:** **Flexibilidade** e **simplicidade** na administração dos direitos de acesso pelos próprios usuários.

- **Desvantagens:** **Menor controle** por parte da organização sobre a distribuição de permissões, o que pode levar a configurações de **segurança menos rigorosas** e potencialmente a vazamentos de informações.

3. MODELO DISCRICIONÁRIO

Fatec Mauá

➢ Controle de Acesso Discricionário (**DAC**)

- No Linux/Unix, cada arquivo e diretório tem um proprietário e um grupo associado. As permissões são definidas separadamente para o proprietário do arquivo, para os membros do grupo e para outros usuários. Os usuários, com as devidas permissões, podem modificar as permissões de um arquivo ou diretório utilizando o comando chmod, mudar o proprietário de um arquivo com chown e o grupo com chgrp. Assim, um proprietário pode ter permissão total, leitura, escrita e execução, enquanto os membros do grupo e outros usuários têm apenas permissão de leitura e execução.

3. MODELO DISCRICIONÁRIO

Fatec Mauá

➢ Controle de Acesso Discricionário (**DAC**)

- No Windows, combinado com ACLs, que são usadas para definir quem pode acessar arquivos e diretórios, bem como o tipo de acesso permitido. Os usuários podem configurar as permissões de acesso através da interface gráfica (clicando com o botão direito no arquivo ou diretório, selecionando "Propriedades" e depois a aba "Segurança") ou utilizando comandos como icacls. Um usuário pode permitir que outro usuário tenha acesso de leitura a um arquivo, mas não de escrita, modificando as permissões na aba de segurança das propriedades do arquivo.

4. MODELO OBRIGATÓRIO

Fatec Mauá

➢ Controle de Acesso Obrigatório (**MAC**)

- **M**andatory **A**ccess **C**ontrol (**MAC**)
  O **MAC** é um modelo mais **restrito**, onde o acesso é **controlado** por um **conjunto de políticas** estabelecidas pela organização e não pelos usuários individuais proprietários dos recursos. Os usuários e recursos são atribuídos a **classes de segurança**, e as políticas determinam as **permissões** ou os **níveis de acesso**. Este modelo é mais usado onde a **segurança da informação** é **crítica**, como em organizações militares ou governamentais.

4. MODELO OBRIGATÓRIO

Fatec Mauá

- Controle de Acesso Obrigatório (**MAC**)

- **Vantagens:** **Alto nível** de controle sobre o acesso aos recursos, com **políticas de segurança** consistentes e centralizadas.
- **Desvantagens:** **Menor flexibilidade** e **maior complexidade** na administração das permissões, podendo resultar em **dificuldades operacionais** para os usuários.

4. MODELO OBRIGATÓRIO

Fatec Mauá

➢ Controle de Acesso Obrigatório (**MAC**)

- No Linux/Unix, por exemplo, a implementação do modelo MAC é o SELinux (Security-Enhanced Linux), que é uma extensão de segurança do Linux, adicionando uma camada mandatória, mais granular e robusta, ao modelo tradicional. Se um arquivo "documento.txt" tiver o rótulo de segurança "secreto", um usuário "Fulano" tiver o rótulo de segurança "confidencial" e a política do SELinux estabelecer que apenas usuários com rótulo "secreto" ou superior podem acessar arquivos rotulados como "secreto", então Fulano não poderá acessar o "documento.txt" devido à política MAC.

5. MODELO BASEADO EM ATRIBUTOS

Fatec Mauá

- Controle de Acesso Baseado em Atributos (**ABAC**)

- **A**ttribute-**B**ased **A**ccess **C**ontrol (**ABAC**)
  O **ABAC** é um modelo **flexível** que utiliza uma ampla gama de **atributos** (características) dos usuários, recursos e/ou ambiente para tomar decisões de controle de acesso. Os atributos podem incluir detalhes como a localização do usuário, a hora do dia, e a sensibilidade do recurso. Este modelo permite uma **granularidade** e **flexibilidade** muito maiores nas definições, com permissões para diversos cenários de uso.

5. MODELO BASEADO EM ATRIBUTOS

Fatec Mauá

- Controle de Acesso Baseado em Atributos (**ABAC**)

- **Vantagens:** **Altamente flexível** e capaz de suportar **políticas** de acesso **complexas** e **dinâmicas**, adaptando-se facilmente a **diferentes cenários** e **necessidades** de negócios.

- **Desvantagens:** **Maior complexidade** na definição e administração das políticas de acesso, exigindo um **entendimento** profundo dos **atributos** e como eles **interagem** entre si.

5. MODELO BASEADO EM ATRIBUTOS

Fatec Mauá

➢ Controle de Acesso Baseado em Atributos (**ABAC**)

- A política de um sistema corporativo de gestão de documentos, segundo o modelo ABAC, por exemplo, se especificar, que: "um usuário com os **atributos** cargo = **"Gerente**" e departamento = **"Financeiro"** e o **atributo** ambiental = "**horário comercial"**, então pode ser acessar documentos com **atributo** classificação = **"Confidencial"**. Neste cenário, ao tentar acessar um documento, o sistema avalia os **atributos do usuário** (cargo e departamento), os **atributos do documento** (classificação) e os **atributos do ambiente** (hora do dia). Se **todos os critérios** forem atendidos, o acesso é concedido; caso contrário, é negado.

6. MODELO BASEADO EM PAPÉIS

Fatec Mauá

➢ Controle de Acesso Baseado em Papéis (**RBAC**)

- **R**ole-**B**ased **A**ccess **C**ontrol (**RBAC**)
  No **RBAC**, os acessos são baseados nos papéis dentro de uma organização, e não na identidade individual dos usuários, para gerenciar direitos e permissões dentro de sistemas de informação. Os **papéis** são atribuídos com base nas funções de trabalho dos **usuários**, e cada papel tem **permissões** específicas. Este modelo facilita a **administração** de permissões, especialmente em organizações **grandes** e **complexas**.

6. MODELO BASEADO EM PAPÉIS

Fatec Mauá

➢ Controle de Acesso Baseado em Papéis (**RBAC**)

- **Vantagens:** **Simplificação** da gestão de acesso, agrupando permissões em papéis. **Flexibilidade** e **escalabilidade,** adaptando-o às mudanças organizacionais. **Segurança** reforçada**,** minimizando riscos com o **princípio** do **menor privilégio**.
- **Desvantagens:** **Complexidade** na **definição** de papéis em ambientes complexos. Gestão **trabalhosa** de papéis dinâmicos, com **mudanças** frequentes. **Dificuldade** de gerenciamento da **granularidade** dos papéis (especificidade e detalhamento).

6. MODELO BASEADO EM PAPÉIS

Fatec Mauá

➢ Controle de Acesso Baseado em Papéis (**RBAC**)

- Um sistema hospitalar estabelece o modelo RBAC para controle de acessos, com as **permissões** para acessar as informações dos pacientes agrupadas em com várias **funções**, por exemplo:

✓ **Médico**: Pode acessar registros médicos completos dos pacientes, escrever prescrições e realizar ordens de exames.

✓ **Enfermeiro**: Tem acesso aos registros médicos dos pacientes, mas não pode escrever prescrições.

✓ **Recepcionista**: Pode acessar informações de contato dos pacientes e agendar consultas, mas não tem acesso aos registros médicos detalhados.

7. MODELO BASEADO EM POLÍTICAS

Fatec Mauá

➢ Controle de Acesso Baseado em Políticas (**PBAC**)

- **P**olicy-**B**ased **A**ccess **C**ontrol (**PBAC**)
  O **PBAC** baseia-se no uso de **políticas formais** de **alto nível** para **definir** e **administrar** controles de acesso. As políticas especificam as **regras de acesso**, que são avaliadas em tempo real para determinar se uma **solicitação** de acesso deve ser **permitida** ou **negada**. Este modelo é útil para implementar **controles** de acesso **complexos** e **dinâmicos** que podem mudar com base em condições externas ou requisitos de negócios.

7. MODELO BASEADO EM POLÍTICAS

Fatec Mauá

➢ Controle de Acesso Baseado em Políticas (**PBAC**)

- **Vantagens:** Permite políticas altamente **granulares**, oferecendo uma **flexibilidade** significativa para **adaptações**. Adequado para atualizações quando os requisitos mudam com frequência. Garantia de **conformidade** com o ambiente regulatório. Possibilita as **decisões** de acesso **contextualizadas**.
- **Desvantagens:** **Complexidade** no entendimento dos requisitos e das capacidades. **Desempenho impactado** por políticas complexas. Riscos de segurança por **definições incorretas**. Dependências de **tecnologias** específicas e necessidade de **especialistas**.

7. MODELO BASEADO EM POLÍTICAS

Fatec Mauá

➢ Controle de Acesso Baseado em Políticas (**PBAC**)

- Uma organização implementa o modelo PBAC para controlar o acesso aos documentos confidenciais. A política leva em conta não apenas o **papel** do usuário, mas também o **contexto** da solicitação de acesso, como a hora e a localização, além de exigir **medidas** de segurança adicionais em determinadas condições, especificando:

✓ **Usuários com o papel de "Gerente"** podem acessar documentos confidenciais de seu departamento das 8h às 18h, dentro do escritório.

✓ **Fora do horário comercial** ou fora do escritório, o acesso requer uma autenticação de dois fatores.

✓ **Usuários com o papel de "Analista"** podem acessar documentos confidenciais apenas quando parte de um projeto específico e somente durante o horário comercial, dentro do escritório.

8. MODELO DE LISTAS DE CONTROLE

Fatec Mauá

➢ Listas de Controle de Acesso (**ACL**)

- **A**ccess **C**ontrol **L**ists (**ACL**)
  As **ACLs** são **listas anexadas** a recursos que **especificam** detalhadamente quais usuários ou sistemas têm **permissão** para **acessar** o recurso e quais **operações** podem realizar. As ACLs são um método ou **mecanismo** usado comumente para **implementar políticas** de controle de acesso, determinando e especificando **configurações** de **direitos** de acesso individuais ou de grupo a objetos de redes, sistemas de arquivos e bancos de dados.

8. MODELO DE LISTAS DE CONTROLE

Fatec Mauá

➢ Listas de Controle de Acesso (**ACL**)

- **Vantagens:** **Controle detalhado** sobre o acesso aos recursos. **Segurança reforçada** contra acessos não autorizados. **Flexibilidade** na aplicação de a uma ampla variedade de recursos. Facilidade no processo de **auditoria** e **conformidade**.
- **Desvantagens:** **Complexidade** no gerenciamento da **infraestrutura**. **Desempenho impactado** em redes de alta velocidade. Riscos de segurança por **definições incorretas**. **Esforço contínuo** para manter as ACLs atualizadas. **Dependência de plataformas**, com diferentes sistemas operacionais e dispositivos de rede.

8. MODELO DE LISTAS DE CONTROLE

Fatec Mauá

➢ Listas de Controle de Acesso (**ACL**)

Exemplos Práticos de Implementação de ACLs

- **Em Sistemas de Arquivos**: Sistemas operacionais como Linux e Windows usam ACLs para definir permissões detalhadas em arquivos e diretórios. Por exemplo, uma ACL pode permitir que o usuário "Fulano" leia e escreva em um arquivo, enquanto outros usuários apenas leiam.

8. MODELO DE LISTAS DE CONTROLE

Fatec Mauá

- Listas de Controle de Acesso (**ACL**)

Exemplos Práticos de Implementação de ACLs

- **Em Redes**: Roteadores e firewalls utilizam ACLs para controlar o tráfego de entrada e saída, baseando-se em critérios como endereços IP de origem e destino, portas e protocolos. Isso ajuda a proteger a rede contra acessos não autorizados e ataques.

8. MODELO DE LISTAS DE CONTROLE

Fatec Mauá

- Listas de Controle de Acesso (**ACL**)

Exemplos Práticos de Implementação de ACLs

- **Em Bancos de Dados**: As ACLs podem controlar o acesso a tabelas, linhas e até colunas específicas dentro de um banco de dados, permitindo que somente usuários autorizados visualizem ou modifiquem dados sensíveis.

SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 04: MODELOS DE CONTROLES DE ACESSO