APRESENTAÇÃO

Segurança da Informação

Controle de Acesso

Jhonatan Geremias (elaboração)

Jhonatan.geremias@pucpr.br

Gonzaga (revisão / atualização)

luis.gonzaga@pucpr.br

Controle de Acesso

- Mecanismo de segurança que permite **limitar ações ou operações** que determinado sujeito (humano ou máquina) pode realizar **sobre** um **recurso**;
- Coexiste com outros serviços de segurança, como o serviço de **autenticação**;
- Utilizado **após** um usuário estar devidamente **autenticado**,
  - Limitará o acesso a usuários **legítimos;**
- Basicamente toda a **segurança da informação depende do controle de acesso**.

Controle de Acesso – (RFC 2828→ RFC 4949 pag. 11)

1. Proteção dos recursos do sistema contra acesso não autorizado.

2. Um processo pelo qual o uso dos recursos do sistema é regulado de acordo com uma política de segurança, e é permitido apenas para entidades autorizadas (usuários, programas, processos ou outros sistemas), de acordo com essa política.

3. Modelo formal - Limitações nas interações entre sujeitos e objetos em um sistema de informação.

4. "A prevenção do uso não autorizado de um recurso, incluindo a prevenção do uso de um recurso de forma não autorizada maneira." [I7498-2] (ISO/IEC 7499-2).

5. EUA Governo - Um sistema que usa recursos físicos, eletrônicos ou controles humanos para identificar ou admitir pessoal com acesso autorizado a um SCIF (*sensitive compartmented information facility* ou recurso de informação sensível compartimentada).

Políticas de Segurança - Controle de Acesso

- Estabelece condições, regras e controles específicos para determinar:
  - Quem pode ter acesso a cada recurso fornecido no sistema;
  - Qual é o tipo de acesso concedido a cada ativo do sistema de informação;
- O controle de acesso faz uma intermediação entre uma entidade e o recurso que esta está tentando acessar, tais como:
  - Sistemas operacionais;
  - Aplicações;
  - Banco de dados, entre outros.

Segurança da Informação - Controle de Acesso

- O **controle de acesso** está estreitamente associado à outras funções relativas à segurança da informação:
  - **Autenticação:** verificar se as credenciais de um indivíduo são válidas;
  - **Autorização**: fornecer permissão a uma entidade (usuário, grupo ou processo) do sistema, permitindo ou restringindo o acesso a algum recurso do sistema.
  - **Auditoria**: garantir que as políticas e procedimentos operacionais sejam devidamente cumpridos;
    - Permitir detectar falhas no processo e na segurança;
    - Solicita mudanças prescrita nos termos de controle, processos e políticas.

Autenticação e Controle de Acesso

- Quando o sistema necessita validar uma entidade que está solicitando acesso.
  - O mecanismo de **autenticação** é utilizado para **determinar se o usuário tem** realmente **permissão** para acessar o sistema;
  - O mecanismo de **controle de acesso** verifica se o **acesso solicitado pelo usuário é permitido.**
    - Ex.: O usuário abre um arquivo e tenta modificar o arquivo;
    - O controle de acesso deve verificar se este usuário tem permissão de escrita nesse este arquivo.

Controle de Acesso - Elementos

- **Sujeito**: Entidade capaz de acessar recursos;
  - **Ex.**: usuário, processo, etc.;
- **Recurso**: Objeto cujo acesso é controlado;
  - **Ex.**: Arquivos, diretórios, páginas, programas, mensagens, etc;
- **Direito de acesso:** Descreve o modo pelo qual um sujeito pode acessar um recurso;
  - **Ex.:** Leitura, Escrita, Execução, Remoção, Criação, Busca, Impressão, etc.

Elementos: Sujeitos

- **Proprietário:** o proprietário é o dono de um recurso, (ex.: diretório, arquivo);
  - Em geral, o usuário responsável em criar determinado recurso automaticamente torna-se proprietário deste recurso;
- **Grupo:** adicional aos privilégios concedidos ao proprietário, um conjunto de usuários pode receber privilégios de acesso por pertencer a um determinado grupo;
  - Um usuário pode se associar a diversos grupos;
- **Outros:** esta categoria se aplica aos usuários autenticados no sistema que não são proprietários e nem pertencem a um grupo de determinado recurso;
  - Concedidos privilégios mínimos de acesso a este recurso.

Elementos: Objeto

- Um objeto é caracterizado como sendo qualquer recurso cujo acesso deve ser controlado.
- O objeto em geral dispõe de alguma informação.
  - Entre alguns exemplos de objeto podemos citar: arquivos, diretórios, programas, mensagens, registros, páginas, entre outros...
  - Em um nível mais baixo alguns sistemas de controle de acesso englobam: bits, bytes, processadores, registradores, portas de comunicação, entre outros...

Elementos – Permissões de Acesso

- **Criar:** permissão que possibilita que os usuários criem tipos de objetos como arquivos, diretórios, registros, instâncias entre outros.
- **Excluir:** permissão que possibilita que os usuários excluam determinados recursos do sistema, tais como arquivos, diretórios, registros, instâncias entre outros.
- **Listar:** permissão que possibilita que os usuários visualizem os recursos, permite listar os arquivos e diretórios do sistema, e ainda realizar buscas nestes diretórios.
- **Ler:** permissão que possibilita que os usuários visualizem informações de um determinado recurso do sistema, incluindo capacidade de copiar ou imprimir. Um exemplo típico é o privilégio de leitura fornecida em um arquivo.

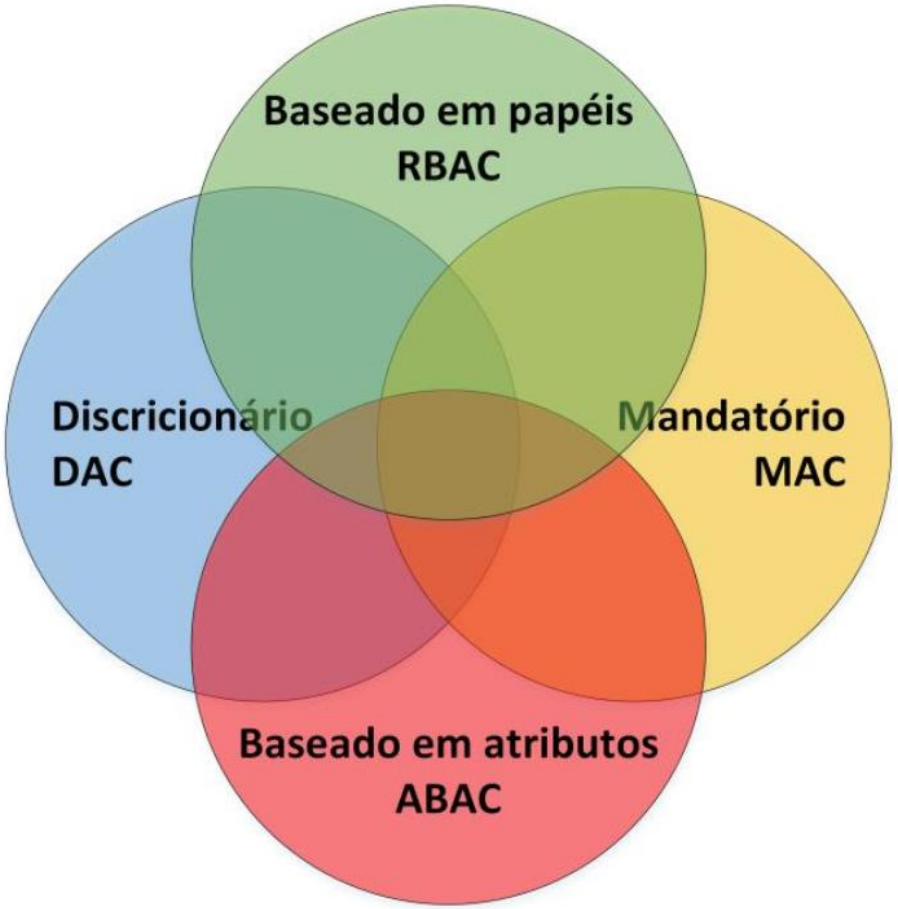
Elementos – Permissões de Acesso

- **Escrever:** permissão que possibilita que os usuários realizem alterações em determinado recurso, podendo incluir, excluir e modificar os dados do sistema. Em muitos casos o acesso de escrita inclui o acesso a permissão de leitura. Ex.: “editar” algum arquivo.
- **Executar:** permissão que possibilita que os usuários executem determinados programas ou rotinas de códigos, em geral programas executáveis ou scripts.

Políticas de Controle de Acesso

- As bases de autorização contém **políticas de acesso**, que determinam o **resultado** da decisão de acesso;
- As políticas mais **tradicionais** são as **discricionárias**, **mandatórias**, **baseadas em papéis** ou em **atributos**;
- É importante ressaltar que essas **políticas não são exclusivas**, ou seja, podem ser **combinadas**.

Políticas de Controle de Acesso



Controle de Acesso Discricionário

- DAC - *Discretionary Access Control*
- Fornece o controle de acesso baseado na identidade do solicitante e em regras de acesso;
- As permissões que definem o que este indivíduo está autorizado a fazer;
- Política nomeada discricionário devido ao fato de uma entidade poder conceder direitos de acesso a outras entidades sobre os recursos que lhe pertence.

Controle de Acesso Mandatório

- MAC – *Mandatory Access Control*
- Política nomeada mandatória (obrigatória);
  - Uma entidade que está autorizada a acessar um certo recurso no sistema **não tem privilégios de conceder acesso** a aquele recurso a outras entidades;
- Fornece o controle de acesso baseado na comparação de **rótulos de segurança** com **autorização de segurança**;
  - Os rótulos de segurança permitem determinar quão crítico são os recursos do sistema;
  - A autorização de segurança permite definir quais entidades do sistema têm permissão para acessar determinados recursos.

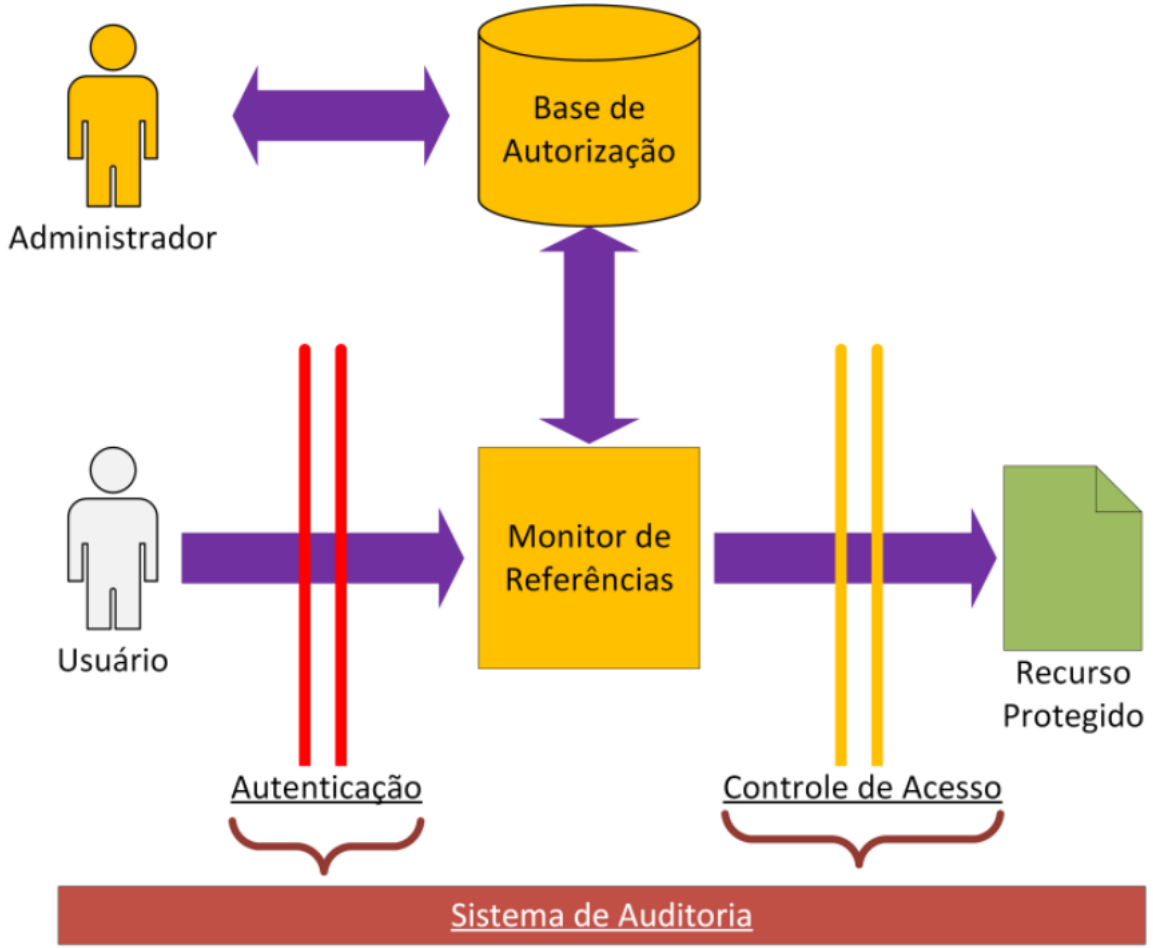
Controle de Acesso Baseado em Papéis

- RBAC - *Role Based Access Control*
- Fornece o controle de acesso baseado nos **papéis** que um indivíduo desempenha dentro do sistema;
- Define regras que **estabelecem quais acessos** podem ser concedidos ao indivíduo que exerce tais **papéis**.

Controle de Acesso - Arquitetura

- **Base de Autorização**: Na forma primitiva, é uma matriz de acesso (sujeito x recurso);
  - Cada célula representa a autorização do usuário sobre o recurso**;**
- **Monitor de Referências**: consulta uma base de autorização para intermediar o acesso de um recurso;
- **Guardião do Recurso (*enforcement*):** Executa a decisão do Monitor, permitindo ou negando o acesso do usuário ao recurso protegido.

Controle de Acesso - Arquitetura



Matriz de Controle de Acesso

- Típica do DAC - Controle de acesso discricionário (*Discretionary Access Control*).
- No DAC uma entidade pode receber privilégios de acesso que permitem que esta entidade habilite outras entidades a acessar certo recurso;
- Em geral, a abordagem implementada pelo DAC é a matriz de acesso;
- Adotada na grande maioria dos sistemas operacionais e SGBD;
- O conceito da matriz de acesso foi proposto por Lampson [LAMPSON, 1969].

Matriz de Acesso

Sujeitos \ Objetos	Arquivo 1	Arquivo 2	Arquivo 3	Diretório 1	Diretório 2
Bob	Proprietário Leitura Escrita		Leitura	Proprietário	Escrita
Alice	Leitura Escrita Execução	Leitura	Proprietário Leitura Escrita	Leitura Escrita	
Jonh	Leitura Escrita	Proprietário Leitura Escrita	Execução		Leitura Escrita
Ted		Leitura Escrita		Leitura	Proprietário Leitura Escrita

Exercício 01

- Desenvolva um programa que realize o controle de acesso. Para isso o programa deve armazenar previamente as políticas.
  - O usuário deve entrar com o login, ação e o recurso no programa, e o sistema deve:
    - Imprimir na tela: “Acesso permitido” caso exista uma política que permita esse acesso.
    - Imprimir na tela: “Acesso negado” caso não exista uma política que permita esse acesso.

Exercício 01

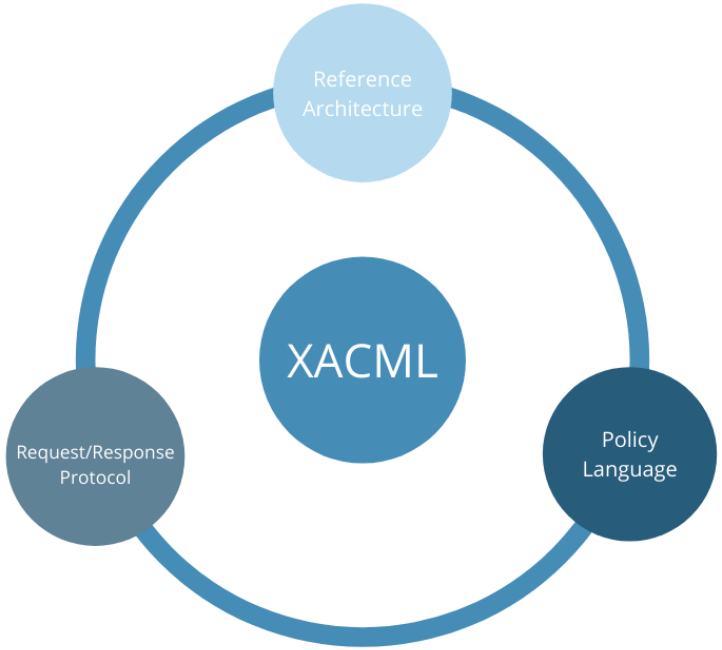
```
matrizAcesso = [ ["",       "Foto.png", "Readme.txt",   "Programa.exe" ],
                 ["vilmar", "read",     "write",        ""],
                 ["maria",  "read",     "",             "execute"],
                 ["pedro",  "read",     "write",        "execute"]]
usuarioDigitado = "vilmar"
acaoDigitada = "read"
recursoDigitado = "Foto.png"
acesso = False
for i in range(1, len(matrizAcesso)):
    usuarioMatriz = matrizAcesso[i][0]
    if usuarioDigitado == usuarioMatriz:
        #O usuario eh valido
        for j in range (1, len(matrizAcesso[0])):
            recursoMatriz = matrizAcesso[0][j]
            if( recursoDigitado == recursoMatriz):
                acaoMatriz = matrizAcesso[i][j]
                if acaoDigitada == acaoMatriz:
                    acesso = True
if( acesso ):
    print("Acesso permitido!")
else:
    print("Acesso negado!")
```

XACML

- O XACML é um popular **framework** de controle de acesso, que define uma **linguagem** baseada em XML para escrita de politicas de controle de acesso, requisições e respostas;
- Adicionalmente, provê um mecanismo de **avaliação** das políticas de controle de acesso;

Exemplo de política

- Abrir o arquivo **[XACML] Politica.xml** pelo navegador.

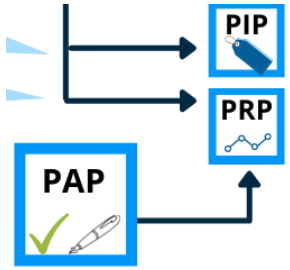


Mecanismo de Avaliação

- O mecanismo de avaliação do XACML é composto dos seguintes elementos:
  - PAP *(Policy Administration Point)*
  - PDP *(Policy Decision Point)*
  - PEP *(Policy Enforcement Point)*
  - PIP *(Policy Information Point)*
  - Context Handler

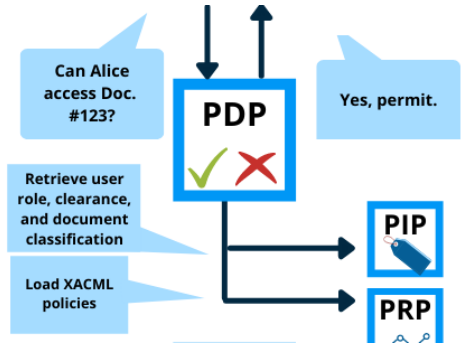
Policy Administration Point (PAP)

- Atua como a **base de autorizações**;
- **Gerencia** e **armazena** as políticas de controle de acesso;



Policy Decision Point (PDP)

- Atua como o **monitor de referências**;
- **Avalia** o pedido de acesso de acordo com as **políticas de controle de acesso** produzindo a **decisão** de acesso (permitido ou negado);

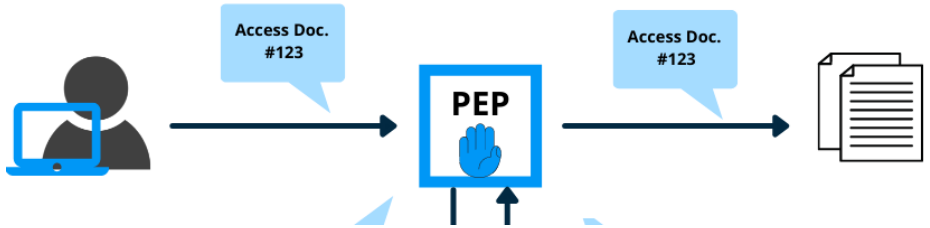


Policy Information Point (PIP)

- Atua como **central de informações**/valores;
- Fornece **informações** (de acordo com as políticas) referentes ao **usuário, recurso** e **ambiente**.

Policy Enforcement Point (PEP)

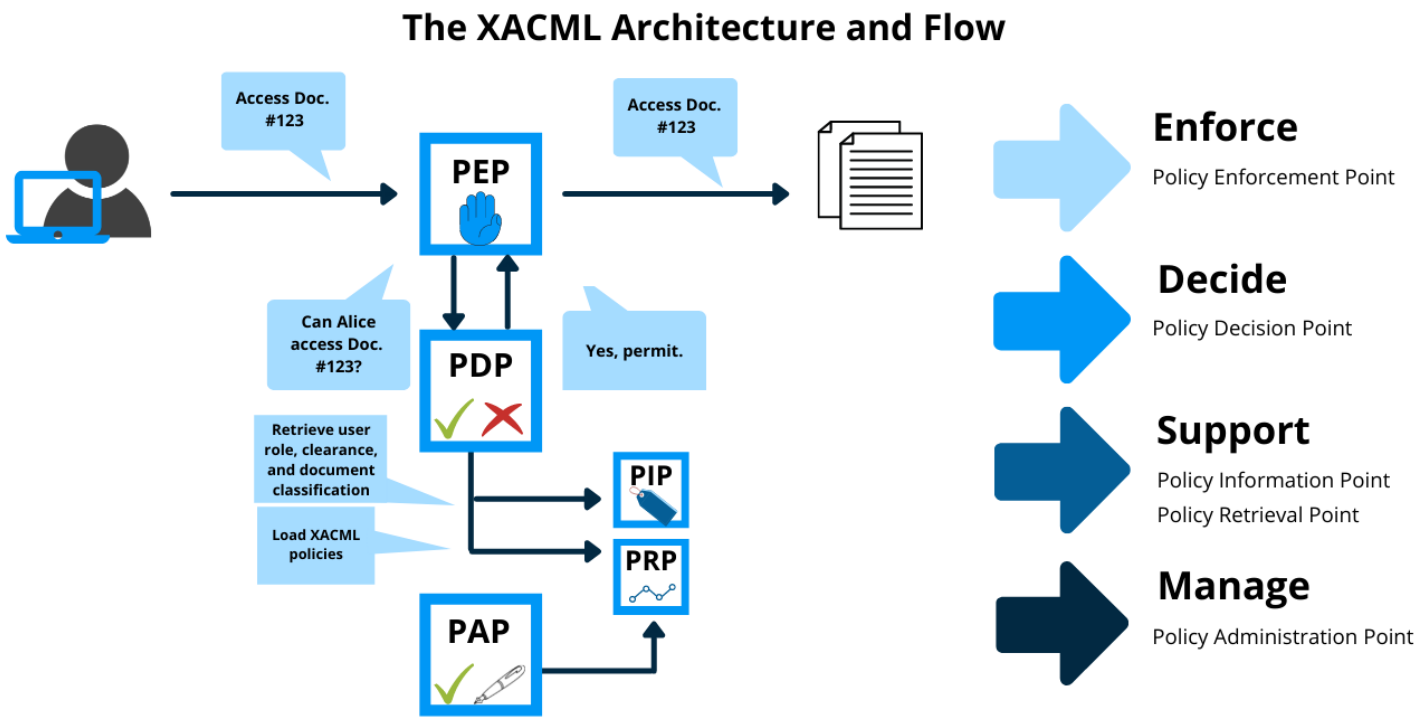
- Atua como a **guardião do recurso**;
- Responsável por **encaminhar os pedidos de acesso** para o PDP, e **conceder o acesso** de acordo com a decisão do PDP;



Context Handler

- Atua como **coordenador**;
- Responsável por realizar a **coordenação, adequação e interoperabilidade** de atributos, requisições e credenciais entre as entidades do XACML.

Arquitetura do XACML



Bibliotecas XACML

- As principais bibliotecas que implementam a especificação do XACML são:
  - Sunxacml (descontinuada)
  - WsO2 Balana

Obrigado!

Jhonatan Geremias (elaboração)

Jhonatan.geremias@pucpr.br

Gonzaga (revisão / atualização)

luis.gonzaga@pucpr.br

SCIENTIA, VITA ET FIDES

PUCPR

GRUPO MARISTA