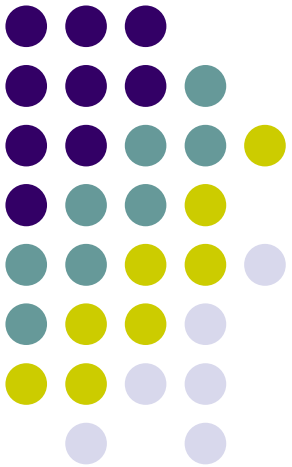
Universidade Federal de São Paulo – UNIFESP

Segurança Computacional

Clique para adicionar texto

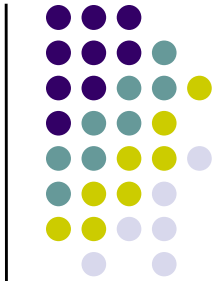
Aula 02 – Políticas de Segurança e Controle de Acesso



Prof. Valério Rosset

Políticas de Segurança

Definição



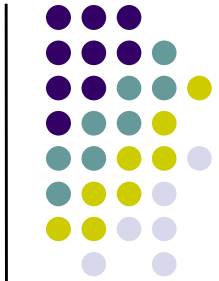
- O termo de política de segurança denota sobre o aspecto organizacional estabelecendo como um sistema deve proceder para difundir ou armazenar informações de maneira segura.

- A política de segurança de um sistema computacional é um conjunto de regras e práticas que determinam como as informações e recursos são geridos, protegidos e distribuídos no interior de um sistema específico.

- Politicas de Segurança Militar vs Comercial

Políticas de Segurança

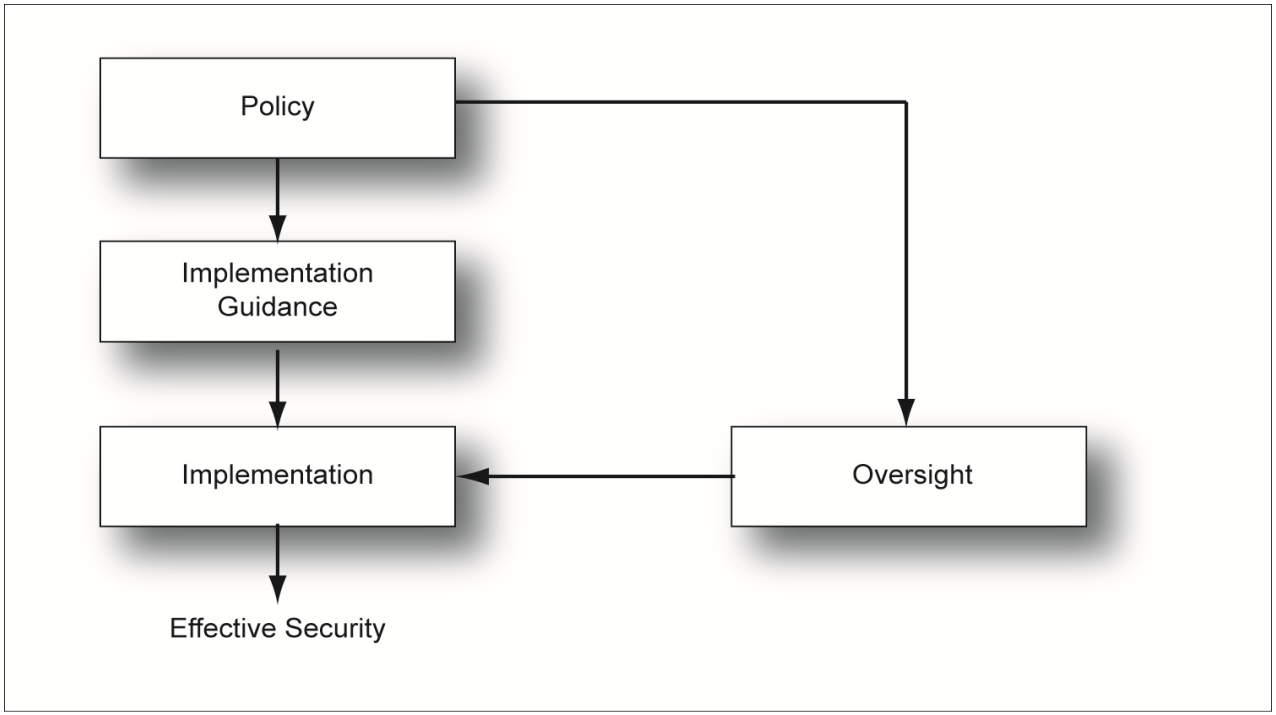
Definição



- Definição do que precisa ser feito
- Provê claresa e direcionamento
- Não especifica em detalhes como a política deve ser implementada

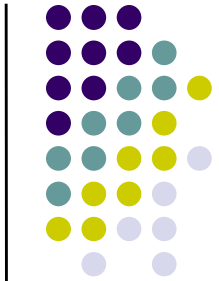
Políticas de Segurança

Ciclo de Implementação



Políticas de Segurança

Orientação de Implementação



Orientação de Implementação

Limita ao disernimento dos implementadores sobre a política para evitar decisões e escolhas ruins.

- **Nenhuma**

O implementador é guiado apenas pela política.

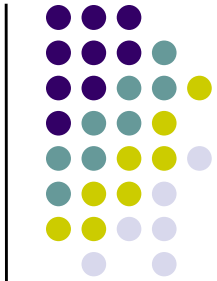
- **Padrões e Diretrizes**

Padrões são deretivas obrigatórias

Diretrizes não são obriagtórias mas devem ser consideradas.

Políticas de Segurança

Supervisão



Supervisão

Um grupo de ferramentas para aplicação da política de segurança.

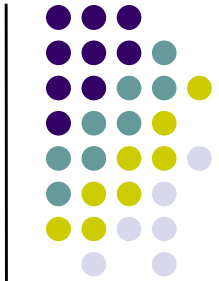
Política guia a Supervisão como também a implementação

Componentes:

- **Disseminação**
- **Monitoramento**
- **Métricas de Segurança**
- **Auditoria**
- **Linha de Apoio Anônima**
- **Teste de Vulnerabilidades**
- **Sanções**

Políticas de Segurança

Definição



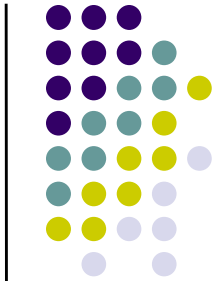
- O termo de política de segurança denota sobre o aspecto organizacional estabelecendo como um sistema deve proceder para difundir ou armazenar informações de maneira segura.

- A política de segurança de um sistema computacional é um conjunto de regras e práticas que determinam como as informações e recursos são geridos, protegidos e distribuídos no interior de um sistema específico.

- Politicas de Segurança Militar vs Comercial

Políticas de Segurança

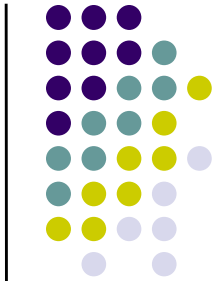
Definição



- Políticas de segurança física
  - As políticas de segurança física determinam como o sistema deve ser protegido fisicamente.
- Políticas de segurança lógica
  - Tratam da segurança das informações que estão armazenadas ou sendo trocadas em um sistema computacional, através de ferramentas e controles internos.
- Ao fim de tudo Treinamento e “Confiança” são Fundamentais.

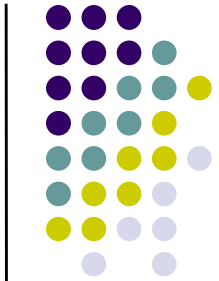
Políticas de Segurança

Definição



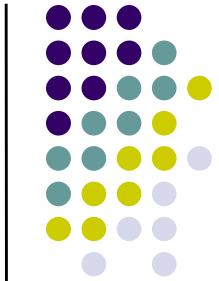
- Políticas de segurança lógica:
  - Políticas de identificação e autenticação
    - Utilizadas para identificar e autenticar usuários de um sistema computacional.
  - Políticas de autorização ou políticas de controle de acesso
    - Depois de identificado o usuário, o sistema deve definir quais ações são autorizadas ao sujeito em particular.

Monitor de Referência & Mecanismos de Segurança



- O ***monitor de referência*** é uma estrutura funcional que toma as decisões referentes a cada requisição de acesso baseado nas políticas de segurança definidas para os usuários de um sistema computacional (Lampson 1971).
- O conjunto de recursos de hardware e software que implementam o conceito de monitor de referência é definido como núcleo de segurança (security kernel).
- A união do núcleo de segurança + controles adicionais de segurança = TCB (*Trusted Computing Base*) definida pelo DoD no livro Trusted Computer System Evaluation Criteria –TCSEC (Orange Book) em 1985.

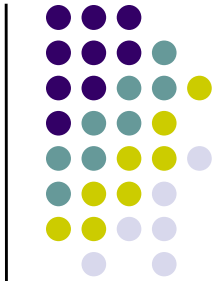
Monitor de Referência & Mecanismos de Segurança



- As funcionalidades de um monitor de referência são implementadas através de mecanismos de segurança.

- Mecanismos de segurança são: criptografia, autenticação e controle de acesso.

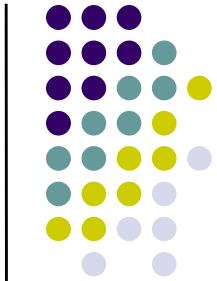
Autorização e Controle de Acesso
Definição



- CONTROLE DE ACESSO
  - Políticas de Autorização Controle de Acesso
  - Modelos de Controle de Acesso
  - Mecanismos de controle de Acesso

Autorização e Controle de Acesso

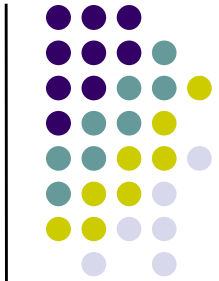
Políticas de autorização e controle de acesso



- São classificadas em:
  - Políticas Discricionárias.
    - Controle de Acesso Discricionário (DAC)
  - Políticas Obrigatórias
    - Controle de Acesso Obrigatório (MAC)
  - Políticas Baseadas em Papéis.
    - Controle de Acesso Baseado em Papéis (RBAC)

Autorização e Controle de Acesso

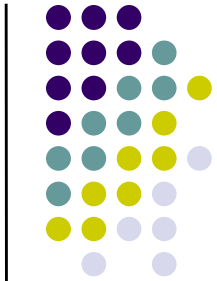
Políticas de autorização e controle de acesso



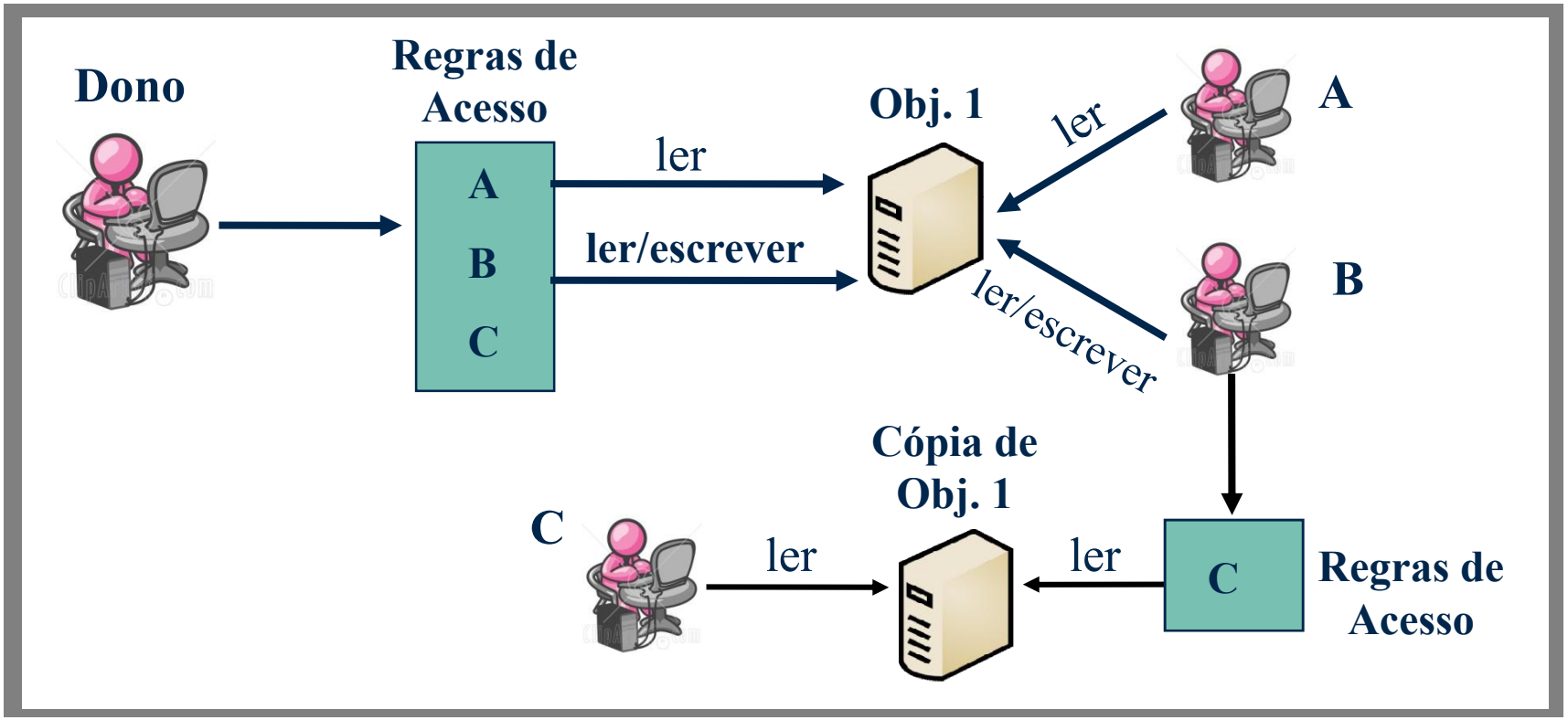
- ***Políticas Discricionárias***
  - Acesso é baseado na identidade do sujeito e em regras de acesso aos objetos.
  - Para cada sujeito (ou grupo) e para cada objeto no sistema, são definidos os modos de acesso específicos que o sujeito possuí sobre um objeto (e.g., leitura, escrita ou execução).

Autorização e Controle de Acesso

Políticas de autorização e controle de acesso

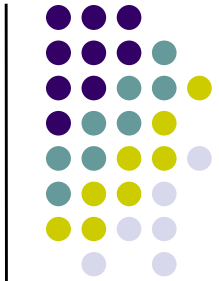


- **Politicas Discricionárias**



Autorização e Controle de Acesso

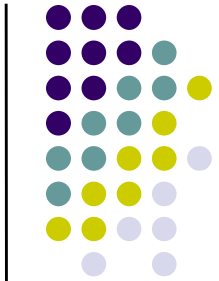
Políticas de autorização e controle de acesso



- ***Políticas Discricionárias***
  - Vantagem: podem ser utilizadas em uma grande variedade de sistemas por sua flexibilidade.
  - Desvantagem: não controlam a disseminação de informação.
    - Por exemplo, sujeitos podem transferir informações restritas a sujeitos não autorizados.

Autorização e Controle de Acesso

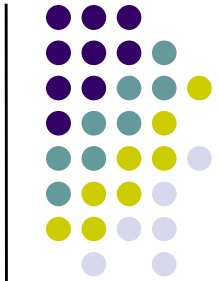
Políticas de autorização e controle de acesso



- ***Políticas Obrigatórias***
  - Baseadas na classificação de sujeitos e objetos em um sistema onde cada sujeito e cada objeto pertencem a um nível de segurança.
  - O nível de segurança a que um objeto pertence determina qual a sensibilidade ou o grau de segurança de uma informação contida nele.
  - Relação hierárquica entre os níveis de segurança associados aos sujeitos definem suas permissões de acesso (*clearance)*, e também que o mesmos não distribuam informação a outros sujeitos que não sejam autorizados a vê-la.

Autorização e Controle de Acesso

Políticas de autorização e controle de acesso

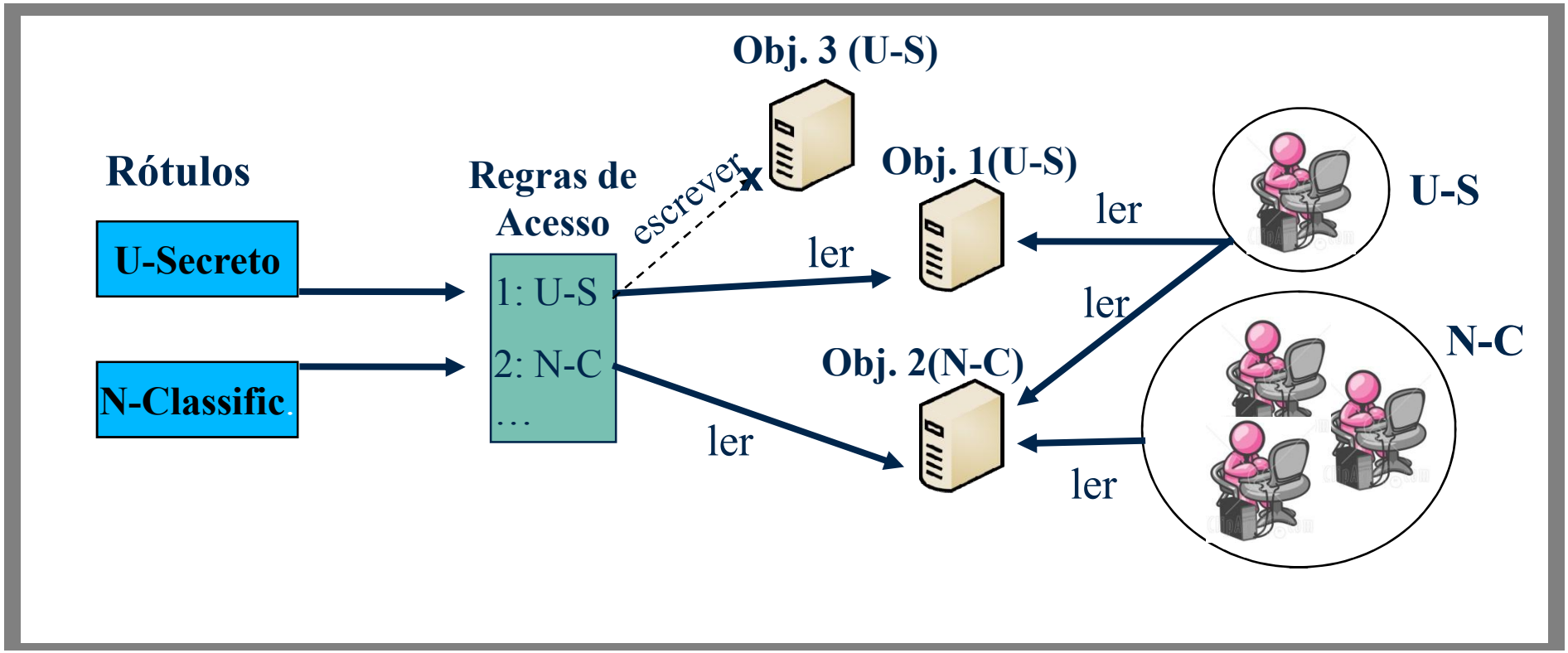


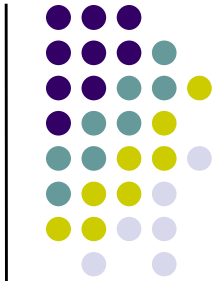
- ***Políticas Obrigatórias***
  - A classificação de sujeitos e objetos é indicada através do uso de etiquetas.
  - O mecanismo utilizado para etiquetar sujeitos e objetos de acordo com a classificação e permissão de acesso é chamado de rótulo de segurança.
  - A autorização do acesso será determinada comparando a permissão de um sujeito com a classificação do objeto.

Autorização e Controle de Acesso

Políticas de autorização e controle de acesso

- **Políticas Obrigatórias**





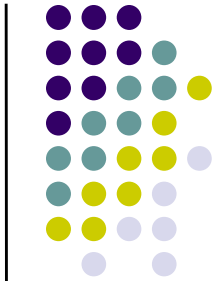
Políticas Obrigatórias

- Vantagem: Controla a disseminação de informações.

- Desvantagem: difícil determinar diferentes direitos de acesso a objetos com mesmo Rótulo de Segurança. Ou seja, é pouco flexível.

Autorização e Controle de Acesso

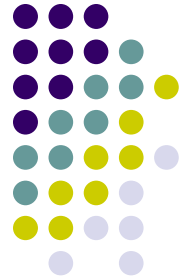
Políticas de autorização e controle de acesso



- ***Políticas Baseadas em Papéis***
  - Definem o acesso às informações com base nas atividades que cada sujeito executa, ou seja, é baseado na função (ou papel) de cada sujeito.
  - Um papel é definido como um conjunto de ações e responsabilidades associadas a uma atividade de trabalho em particular.

Autorização e Controle de Acesso

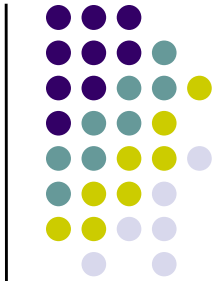
Políticas de autorização e controle de acesso



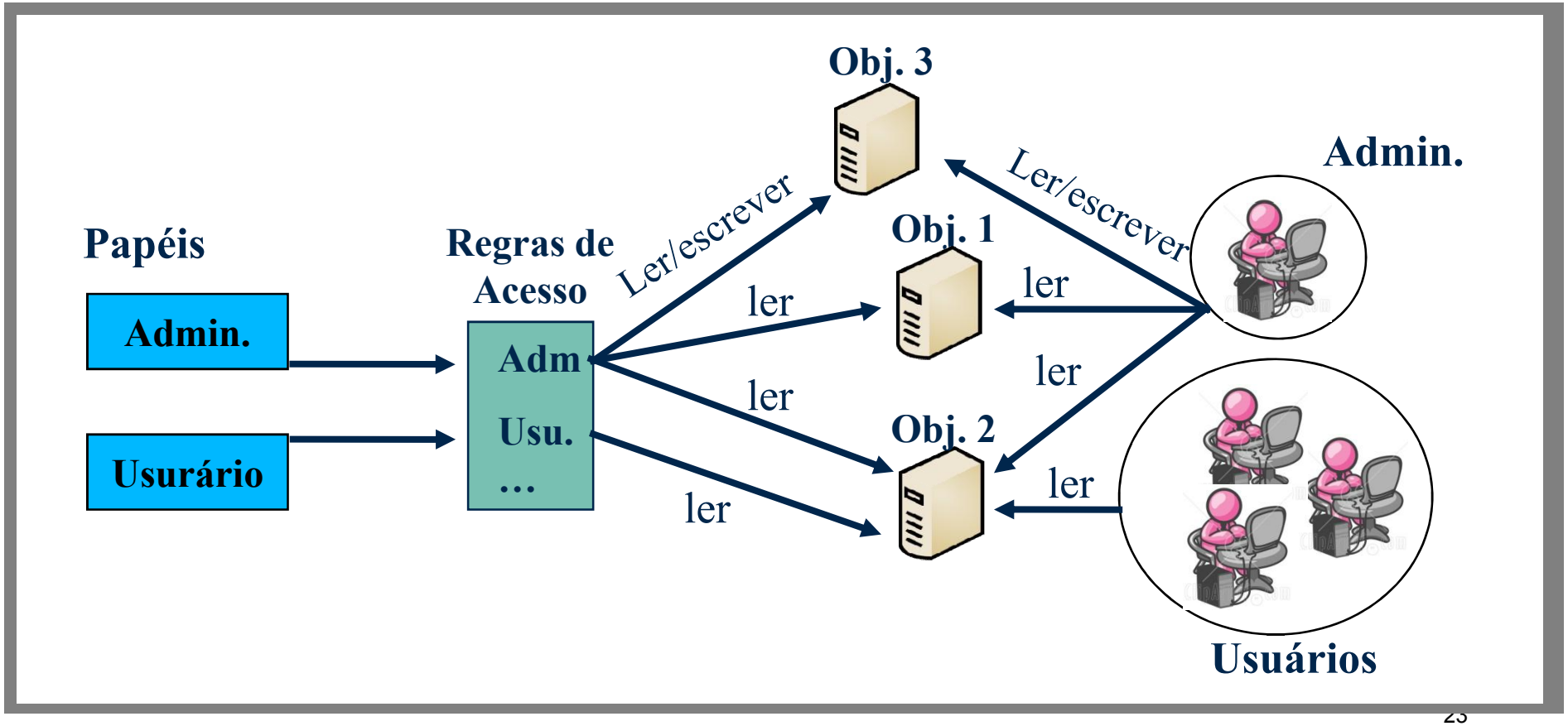
- ***Considerações sobre políticas baseadas em papéis***
  - Sujeito:
    - É atribuído um determinado papel e tem permissão para executar operações para as quais esse papel é autorizado.
    - É possível determinar que vários sujeitos exerçam o mesmo papel.
  - Objetos:
    - São associados a uma classe, vários objetos podem pertencer a uma única classe.
    - O sujeito tem permissão para acessar não só um objeto específico, mas também qualquer objeto que pertença à mesma classe.

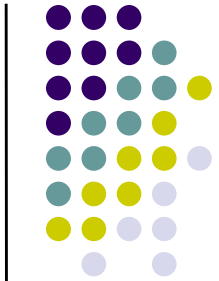
Autorização e Controle de Acesso

Políticas de autorização e controle de acesso



- **Políticas Baseadas em Papéis**



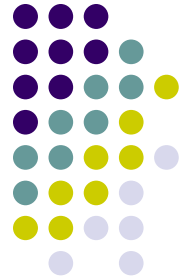


Políticas Baseadas em Papéis

- Vantagem: Controla a disseminação de informações ao mesmo tempo que permite a definição de diferentes direitos de acessos a objetos da mesma classe.
- Desvantagem: Não permite a definição de direitos de acesso individualmente a sujeitos (em muitos casos não pode ser considerado uma desvantagem).

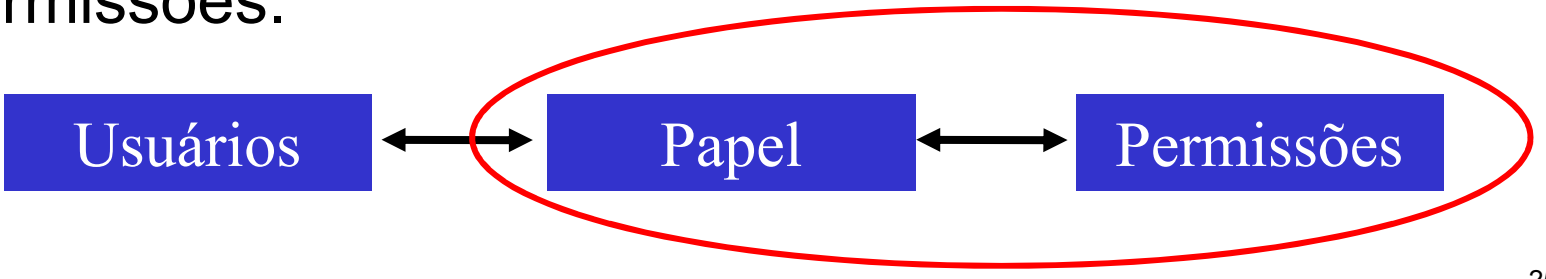
Autorização e Controle de Acesso

Políticas de autorização e controle de acesso



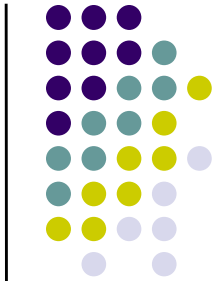
- ***Diferenças – Grupos de Usuários e Papéis***
  - Grupos (são coleções de usuários): onde as permissões são definidas para cada grupo ou usuário individualmente.

  - Papéis: são únicos e associados a uma coleção de permissões.



Autorização e Controle de Acesso

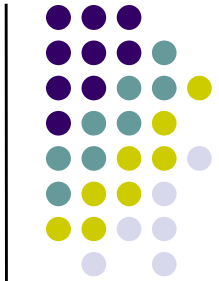
Modelos de Controle de Acesso



- Um Modelo de Controle de Acesso determina a implementação das políticas de controle de acesso para um sistema.
- Modelos de Controle de Acesso são formas de descrever as políticas de autorização, determinando tanto o comportamento de entidades governadas pela política quanto às regras que definem a evolução desta política.

Autorização e Controle de Acesso

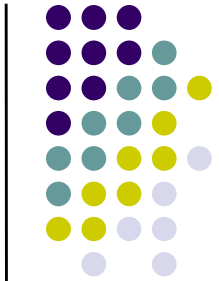
Modelos de Controle de Acesso



- ***Modelo BLP - Bell e La Padula [1976]***
  - O conceito de controle de acesso obrigatório (MAC) foi formalizado primeiramente no modelo Bell-La Padula (BLP).
  - O modelo BLP une as características de um controle de acesso discricionário com o controle de acesso obrigatório, para a implementação das políticas de segurança que controlam o fluxo de informações em um sistema.
  - Essas políticas são chamadas políticas de Segurança Multinível (MLS). Onde usuários podem apenas acessar informações em nível de segurança igual ou inferior ao que lhe é permitido.

Autorização e Controle de Acesso

Modelos de Controle de Acesso

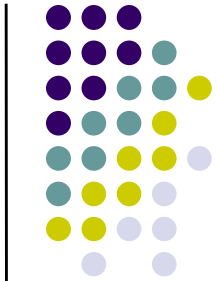


- O modelo BLP foi desenvolvido utilizando os princípios de Máquina de Estados, onde cada estado seguro precisa satisfazer duas propriedades básicas de segurança.
  - No-Read-Up e No-Write-Down

- BLP foi desenvolvido para ambientes onde os direitos de acesso são estáticos e os objetos não mudam seu nível de segurança.

Autorização e Controle de Acesso

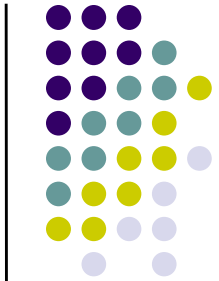
Modelos de Controle de Acesso



- ***Modelo RBAC (Role-Based Access Control)***
  - A utilização dos conceitos de políticas baseadas em papéis é a principal característica do modelo de segurança RBAC .
  - Promove suporte aos princípios de segurança organizacional como:
    - O privilégio mínimo (*least privilege*): determina que a um papel são atribuídos apenas os direitos mínimos necessários para a realização das tarefas referentes ao papel.

Autorização e Controle de Acesso

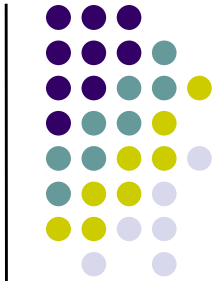
Modelos de Controle de Acesso



- A separação de deveres (*separation of duties-SoD*): determina que haja a existência de papéis de forma conjunta na execução de determinadas operações. Por exemplo, a existência de um funcionário realiza a emissão de cheques somente com autorização de um gerente contábil.

Autorização e Controle de Acesso

Modelos de Controle de Acesso



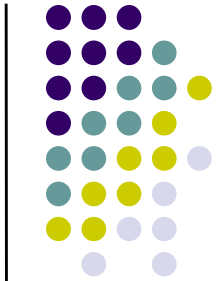
- ***Outros Modelos***

- Confidencialidade de informações
  - Modelo Chinese Wall [1989] considera mudanças dinâmicas dos direitos de acesso.
    - (Ninguém vê o que está do outro lado da parede).

- Integridade de informações, contra modificação não autorizada, fraudes e erros.
  - Biba [1977].
  - Modelo Clark-Wilson [1987].
    - **SoD e Well Formed Transactions**

Autorização e Controle de Acesso

Mecanismos de Controle de Acesso

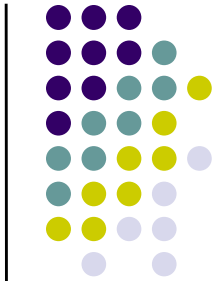


- ***Matriz de Controle de Acesso***
  - A matriz de controle de acesso é um modelo conceitual utilizada para descrever direitos de acessos.

Objetos / Sujeitos	Arquivo 1	Arquivo 2	Arquivo 3	Prog.X
Ana	Ler, escrever	Ler	Dono	Executar
Maria	-	Dono	Ler	-
João	Dono	-	Ler, escrever	-
Prog. X	Ler	Ler	-	-

Autorização e Controle de Acesso

Mecanismos de Controle de Acesso

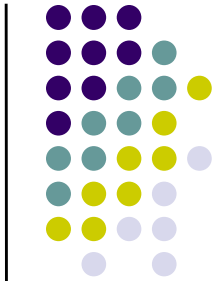


- Acesse em Sistemas de Arquivos baseados em Unix.
  - bits são detalhados a seguir:
  - Bit 8 - leitura pelo proprietário
  - Bit 7 - escrita pelo proprietário
  - Bit 6 - execução pelo proprietário
  - Bit 5 - leitura pelos membros do grupo
  - Bit 4 - escrita pelos membros do grupo
  - Bit 3 - execução pelos membros do grupo
  - Bit 2 - leitura por outros usuários do sistema
  - Bit 1 - escrita por outros usuários do sistema
  - Bit 0 - execução por outros usuários do sistema

- ***drwxr-xr-x 2 root root 4096 Nov 20 06:33 bin***
- ***drwxr-xr-x 3 root root 4096 Nov 20 06:34 boot***
- ***drwxr-xr-x 14 root root 4000 Nov 19 15:59 dev***

Autorização e Controle de Acesso

Mecanismos de Controle de Acesso



- Lista de controle de acesso (Access Control List - ACL)
  - Armazena os direitos de acesso separadamente para cada objeto.

Arquivo 1 : Ana(ler , escrever), João(dono) …

Arquivo 2 : Ana (ler), Maria (dono) , Programa X (ler)

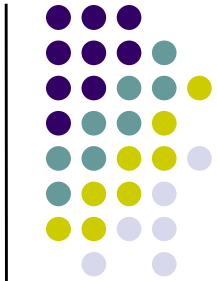
Arquivo 3 : Ana(dono), Maria (ler), João(ler, escrever)

Prog. X : Ana (executar)

- **Permite fácil visualização/revogação de todos os direitos de acesso sobre um objeto.**
- **Maior esforço em determinar os direitos de cada usuário**

Autorização e Controle de Acesso

Mecanismos de Controle de Acesso

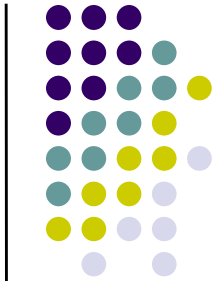


- ***Capabilities (habilitações)***
  - Definem os direitos de acesso (linha da Matriz CA) sobre objetos baseados em tokens persistentes de acesso como um ticket ou chave.
  - Sujeito possui uma habilitação que pode ser repassada a outros sujeitos (não necessita autenticação).
  - Tem prazo de validade (Ex. Cookies)

> **➢ Permite fácil visualização/revogação de todos os direitos de acesso a um objeto.**
>
> **➢ Muito esforço para controlar o acesso de sujeitos específicos.**
>
> **➢ Maior esforço em determinar quem tem acesso a cada objeto.**

Autorização e Controle de Acesso

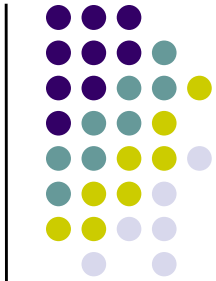
Mecanismos de Controle de Acesso



- ***Rótulos de segurança***
  - Um rótulo de segurança é um atributo associado a objetos que determina seu grau sensibilidade.
  - O rótulo de segurança consiste em dois componentes:
    - nível de segurança e categoria de segurança.
  - O acesso é concedido aos sujeitos através de uma permissão (clearence) = Nível de segurança + Categoria
  - Os níveis de segurança (**MAC**):
    - *NÃO-CLASSIFICADO < CONFIDENCIAL < SECRETO < ULTRA-SECRETO*
  - Categorias:
    - Informativo < Permissivo < Restritivo

Autorização e Controle de Acesso

Mecanismos de Controle de Acesso



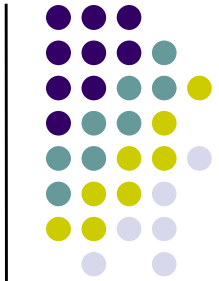
- Rótulos de segurança

Objeto	Nível de Segurança	Categoria
Arquivo 1	Ultra-Secreto	**Restritiva (A,B)**
Aqruivo 2	Ultra-Secreto	Permissiva(A,B)

Sujeito	Nível de Segurança	Categoria
João	Ultra-Secreto	A,B

Sujeito	Nível de Segurança	Categoria
Maria	Ultra-Secreto	A

Tarefa 01



- Pesquise e escreva um resumo sobre novos tipos de controle de acesso abaixo, indicando quais suas características e modo de funcionamento, com exemplos:
  - Attribute-based access control
  - Break-Glass Access Control Models
- Tarefa é individual.
  - Máximo 3 Páginas.