Proteção de Objetos em S.O.

Vinícius da Silveira Serafim

professor@serafim.eti.br

Sistemas Operacionais

- Dois objetivos (PFLEEGER 2006, p. 188)
  - Controlar acesso compartilhado
  - Implementar uma interface para permitir o acesso
- Ampla variedade
  - mono (usuário, tarefa)
  - multi (usuário, tarefa)

Sistemas Operacionais

- Ampla variedade
  - mono (usuário, tarefa)
  - multi (usuário, tarefa)
- Exemplos
  - Smartcards (Chip Operating System)

  - Android (Goolge) e IOS (Apple)
  - Microsoft, Linux, Mac OS X

Sistemas Operacionais

- Mono
  - Proteção do S.O.
- Multi
  - Proteção de programas e dados do usuário
  - memória, dispositivos de I/O, redes, dados e programas compartilhados,...

Metodos de Segurança

- Base para proteção: **Separação**
  - Manter os objetos de um usuário separados de outros usuários
- Pode ser obtida de diversas formas
  - Separação física
  - Separação temporal
  - Separação lógica
  - Separação criptográfica

Separação e Compartilhamento

- Separação não é tudo
- É desejado algum nível de **compartilhamento** de objetos entre usuários
  - O que torna o controle mais complicado

Diversos Níveis de Proteção

- Sem proteção
- Isolamento: cada processo é completamente isolado dos demais
- Compartilhamento "tudo ou nada": ou um objeto é público ou é privado
- Compartilhamento via limitação de acesso: permissões por usuário a um objeto
- Limitação do uso de um objeto: limita não só o acesso mas o uso que pode ser feito

Granularidade

- O controle de acesso pode ser realizado em vários níveis
  - bit
  - byte
  - registro
  - arquivo
  - volume

Controle de Acesso à Objetos

Quais objetos?

- Alguns exemplos
  - memória
  - arquivos
  - um programa em execução
  - diretório de arquivos
  - dispositivo de hardware
  - senhas

Diretório

- Cada sujeito tem um diretório
- Cada diretório lista os arquivos aos quais cada sujeito tem direitos de acesso (leitura, execução, escrita e dono)
- Problemas
  - Listas aumentam rapidamente se muitos objetos forem compartilhados
  - Revogação de acesso

Listas de Controle de Acesso

- ACL (Access Control Lists)
  - Uma ACL por objeto
    - Permissões para sujeitos específicos
    - Permissões padrão (default)

Em Resumo

- Diretórios
  - "Uma lista de objetos acessíveis por um determinado sujeito"
- ACL
  - "Uma lista de sujeitos que podem acessar um determinado objeto"