Um modelo de segurança para proteger arquivos pessoais

Evandro Fernandes Giovanini
Supervisor: Marco Dimas Gubitoso

16 de novembro de 2015

Introdução

O Unix foi pensado em outra realidade (1969)

- Muitos usuários compartilhavam acesso a poucos computadores
- Objetivo: Proteger o sistema contra usuários maliciosos
- Objetivo: Proteger usuários de outros usuários
- Aplicativos instalados por administradores

Introdução

Hoje o cenário é outro

- Usuários são responsáveis por seus próprios computadores
- Instalam programas e baixam arquivos de fontes não confiáveis
- A proteção do sistema a esse cenário é praticamente inexistente.

Exemplos

Programas maliciosos

- rm -rf /

Este comando não prejudica a instalação do SO, "só" apaga todos os arquivos do usuário!

Exemplos

Programas maliciosos

- netcat

Um programa qualquer pode enviar todos os dados pessoais para um servidor remoto.
Esses exemplos podem ser explorados em qualquer aplicativo.

Introdução ao funcionamento

SecApp: cada aplicativo tem um diretório pessoal próprio.

Estrutura de diretórios

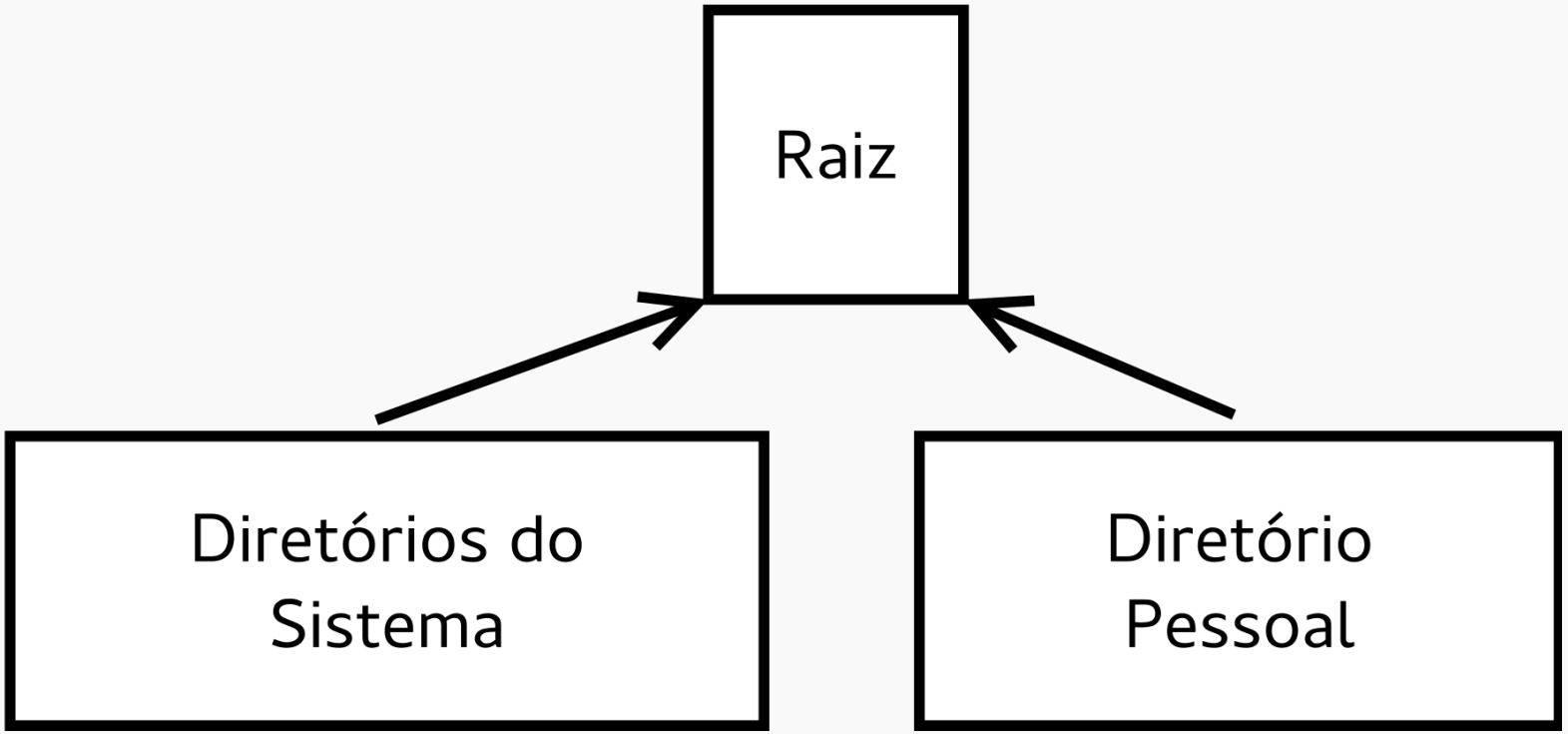

Figure: Estrutura de diretórios

Estrutura de diretórios

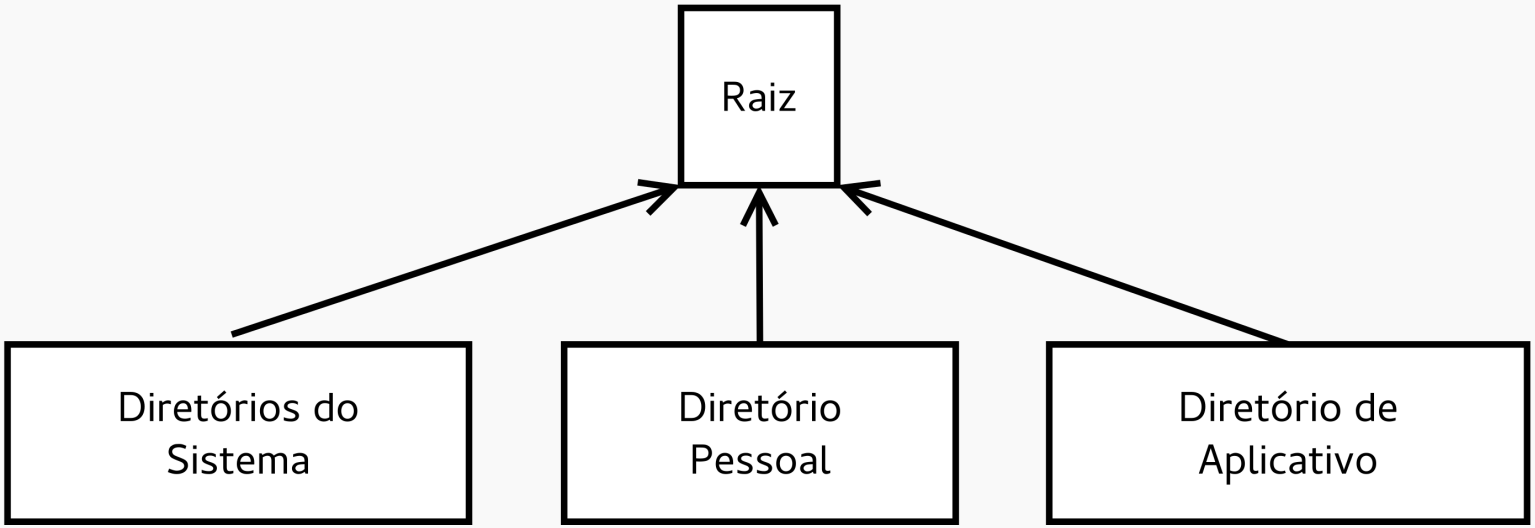

Figure: Estrutura de diretórios

Estrutura de diretórios

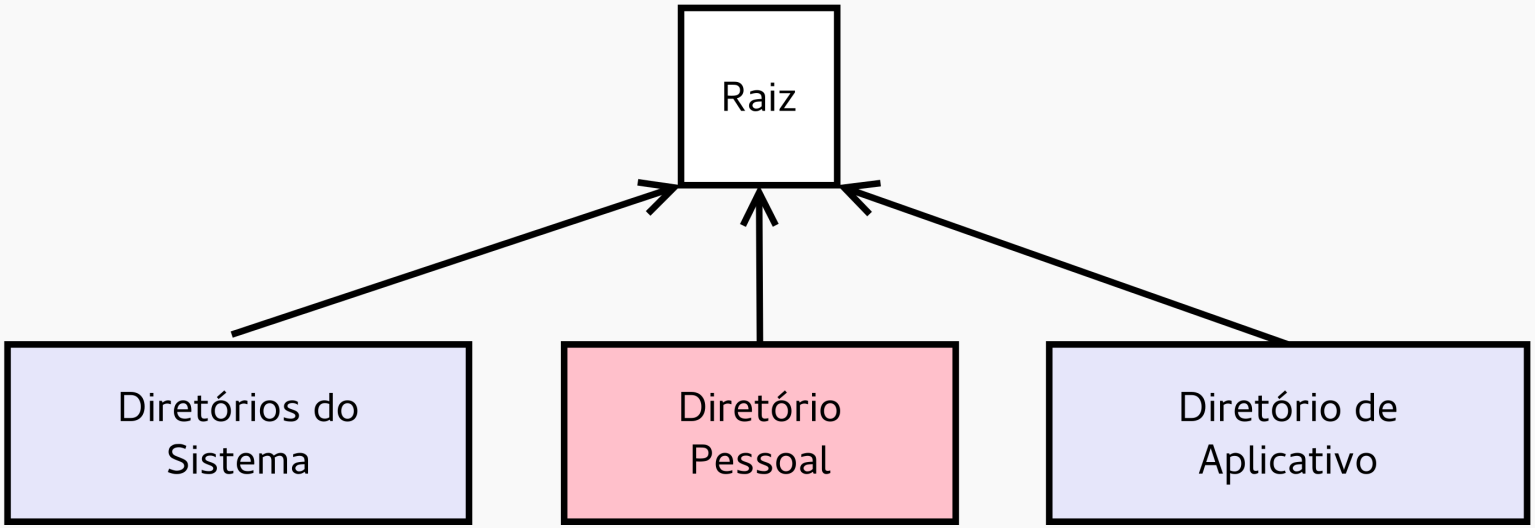

Figure: Estrutura de diretórios

Exemplo

Exemplo de funcionamento

secapp-run /usr/bin/firefox

- O SecApp cria o ambiente de execução para o Firefox
- Faz um *chroot jail* nesse ambiente de execução
- Então inicia o aplicativo dentro da *chroot jail*

chroot jail

Um aplicativo só consegue escapar da *chroot jail* com permissões de root Assim, a segurança padrão do Unix é suficiente para impedir isso.

Concedendo permissões

As vezes o usuário quer enviar pelo Firefox um documento criado no Libreoffice.

Como acessar arquivos de outros aplicativos?

Secappd

Secappd é um *daemon* que roda na sessão do usuário, com acesso normal a todos arquivos

- Aplicativos pedem permissão de leitura ao secappd
- O secappd pergunta ao usuário se deseja conceder acesso
- Caso permitido, o secappd disponibiliza os arquivos ao aplicativo

Secappd - detalhes

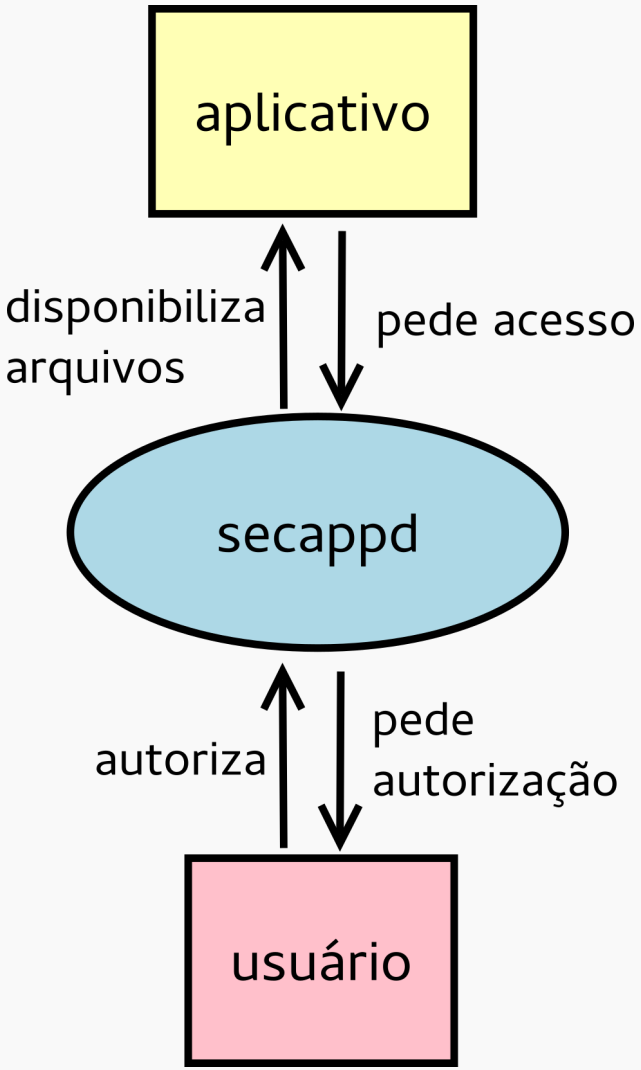

Figure: secappd

Overlayfs

- Os arquivos são disponibilizados pelo *overlayfs*
- O diretório pessoal real e o diretório específico do aplicativo são sobrepostos
- Os arquivos do diretório pessoal real apenas são lidos, modificações são escritas no diretório específico do aplicativo

Conclusão

- O SecApp pode ser usado para isolar aplicativos
- Permite acesso a arquivos quando necessário