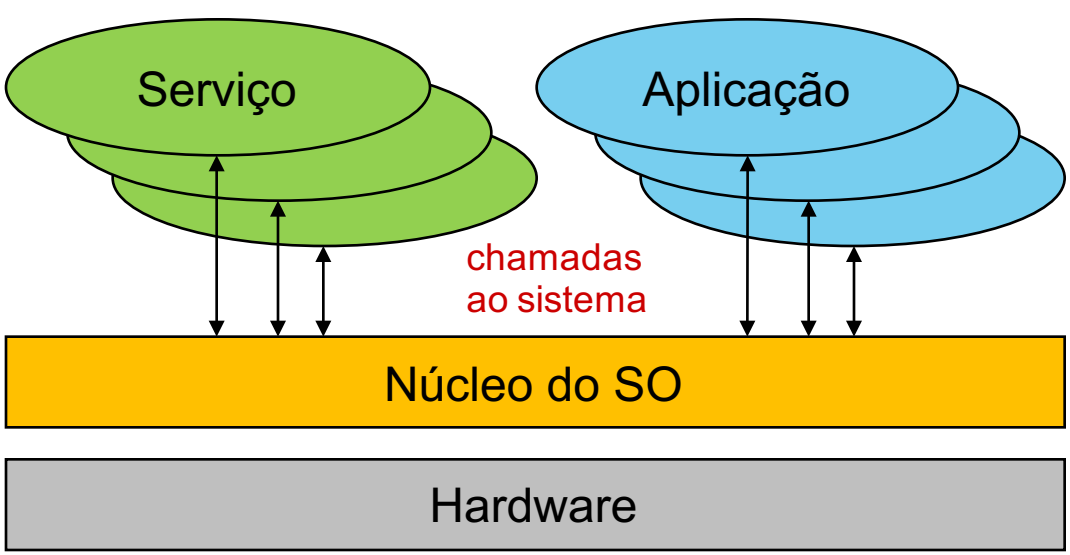
Segurança em Sistemas Operativos

Sistema Operativo



user-mode:

Executa no modo normal do CPU,
Sem instruções privilegiadas

supervisor mode:

Executa no modo privilegiado do CPU,
Com instruções privilegiadas

Objetivos do Núcleo do SO

Inicializar o dispositivos de hardware (booting)

Virtualizar o hardware, fornecendo um interface para as aplicações

- Modelo computacional

Aplicação das políticas de proteção e fornecimento de mecanismos de proteção

- Contra enganos involuntários
- Contra atividades não autorizadas

Fornecer um Sistema de Ficheiros Virtual (VFS)

Modos de execução

Diferentes níveis de privilégio

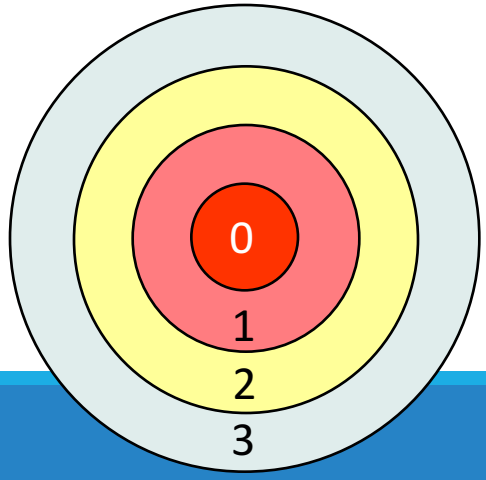
- Normalmente ilustrados por um conjunto de anéis concêntricos
- Usados em CPU's para evitarem que aplicações não privilegiadas executem instruções privilegiadas
  - e.g. IN/OUT, gestão de TLB

Os processadores atuais têm 4 anéis

- Mas os SO's normalmente só usam 2
  - 0 (modo supervisor) e 3 (modo utilizador)

A transferência de controlo entre anéis requer mecanismos de passagem especiais

- Os quais são usados pelas system calls



Execução de Máquinas Virtuais

Aproximação típica

- Virtualização baseada em Software
- Execução direta de código em modo de utilizador (anel 3)
- Tradução binário de código privilegiado (anel 0)

Virtualização assistida por hardware

- Virtualização completa (Full)
- Utiliza-se anel -1, abaixo do anel 0
  - Intel VT-x e AMD-V
- Virtualisador consegue executar vários SOs em nível 0
  - Sem necessidade de tradução binária
  - Com performance próxima da nativa

Modelo computacional

Conjunto de entidades (objetos) geridos pelo núcleo do SO

- Identificadores de utilizadores
- Processos
- Memória virtual
- Ficheiros e sistemas de ficheiros
- Canais de comunicação
- Dispositivos físicos
  - Suportes de armazenamento
    - Discos magnéticos, óticos, de memória, cassetes
  - Interfaces de rede
    - Com fio, sem fio
  - Interface humano-computador
    - Teclados
    - Ecrãs
    - Ratos
  - Interfaces I/O série/paralelo
    - Barramentos USB, portas série, portas paralelas, infravermelhos

Modelo computacional: Identificadores de utilizadores

Para um SO um utilizador é um número

- Estabelecido durante a operação de login
- User ID (UID)

As atividades executadas num computador fazem-se sempre associadas a um UID

- O UID permite estabelecer o que é permitido/negado às atividades
- Em Linux o UID 0 é omnipotente (root)
  - A administração da máquina é normalmente feita recorrendo a atividades com o UID 0
- Em Windows existe o conceito de privilégios
  - De administração, de configuração do sistema, etc.
  - Não existe um identificador único e bem estabelecido para um administrador
  - Os privilégios de administração podem ser dados a diversos UIDs

Modelo computacional: Identificadores de grupos

Também existem identificadores de grupo

- Um grupo é um conjunto de utilizadores
- Um grupo pode ser definido à custa de outros grupos
- Group ID (GID)

Um utilizador pode pertencer a diversos grupos

- Os seus privilégios são determinados através do conjunto de privilégios atribuídos a si e aos grupos a que pertence
  - Direitos = Direitos UID + Direitos GIDs

Em Linux as atividades executadas fazem-se sempre associadas a um conjunto de grupos

- Grupo primário
  - Normalmente usado para definir proteções de novos ficheiros
- Grupos secundários
  - Usados, juntamente com o anterior, para definir se se tem ou não acesso a recursos

Modelo computacional: Processos

Um processo contextualiza uma atividade

- Para efeitos de decisões de segurança
- Para outros fins

Contexto com relevância para a segurança

- Identidade (UID e GIDs)
  - Fundamental para efeitos de controlo de acesso do processo
- Recursos atualmente em uso
  - Ficheiros abertos
    - Incluindo canais de comunicação
  - Áreas de memória virtual reservadas
  - Tempo de CPU usado

Memória virtual

É um espaço de memória onde têm lugar ações efetuadas por uma atividade

- Tem uma dimensão máxima que é definida pela arquitetura de hardware
  - 32 bits → 232 B (4 GB) máximo
  - 64 bits → 264 B máximo

A memória virtual não precisa (e normalmente não pode) ser usada na íntegra

- Apenas é usada uma parcela (a necessária)

A memória virtual é mapeada em memória física (RAM) quando é necessário nela ler ou escrever

- Num dado instante, a memória física possui partes de várias memórias virtuais
- A escolha automática dessas partes é uma das funções mais importantes de um SO

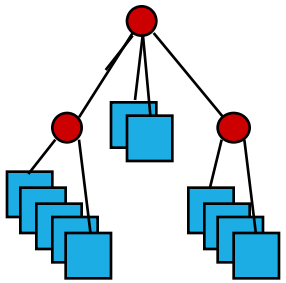
Modelo computacional: Ficheiros e sistemas de ficheiros

Ficheiros

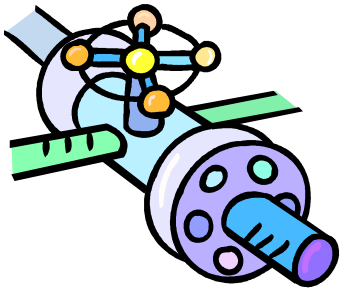
- Servem para armazenar dados de forma perene
  - Mas a longevidade é dada pelo suporte físico e não pelo conceito de ficheiro …
- São sequências ordenadas de bytes associadas a um nome
  - O nome permite recuperar/reutilizar esses bytes mais tarde
- O seu conteúdo pode ser alterado, removido, ou acrescentado
- Possuem uma proteção que controla o seu uso
  - Permissões de leitura, escrita, execução, remoção, etc.
  - O modelo de proteção depende do sistema de ficheiros

Sistemas de ficheiros

- São estruturas hierárquicas de arrumação de ficheiros
- São formados por diretorias (nós) e ficheiros (folhas)
- As diretorias também possuem nome
- A diretoria no topo é a raiz do sistema de ficheiros



Modelo computacional: Canais de comunicação



Permitem a troca de dados entre atividades distintas mas cooperantes

- Processos do mesmo SO/máquina
  - Pipes, Sockets UNIX, streams, etc.
- Processos em máquinas distintas
  - Sockets TCP/IP e UDP/IP

Mecanismo essencial para operação de um sistema

Modelo computacional: Proteção com ACLs

Lista de controlo de acesso (Access Control List, ACL)

- Cada "objeto" possui uma ACL
  - Diz quem pode fazer o quê
  - Entidade → direito de operação

A ACL pode ser discricionária ou obrigatória (mandatory)

- Quando é obrigatória não se consegue contornar
  - É fixada pelo seu criador
- Quando é discricionária pode ser alterada
  - Pelo dono do objeto

É verificada quando uma atividade pretende manipular o "objeto"

- Se o pedido de manipulação não estiver autorizado é negado
- Quem faz as validações das ACLs é o núcleo do SO
  - Monitor de segurança

Controlo de acesso obrigatório

Existem inúmeros casos de controlo de acesso mandatório num sistema operativo

- São mecanismos de controlo embebidos na própria lógica do modelo computacional do sistema operativo e que não são moldáveis pelos utentes e administradores

Exemplo: envio de sinais (signals) entre processos Unix

- Apenas root ou ou mesmo UID o pode fazer
- Não há qualquer controlo sobre esta funcionalidade

Proteção de ficheiros no Linux: ACLs de dimensão e estrutura fixa

Cada elemento do sistema de ficheiros possui uma ACL

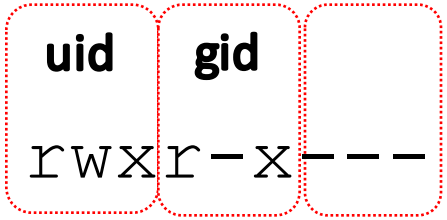
- Atribui 3 tipos de direitos a 3 entidades
- Apenas o dono do elemento pode mudar a ACL

Direitos: R W X

- Para os ficheiros normais significam direito de:
  - Leitura
  - Escrita
  - execução
- Para as diretorias significam direito de:
  - Listagem
  - Adição/remoção de ficheiros ou subdiretorias
  - Uso como diretoria corrente do processo

Entidades:

- Um UID (dono do ficheiro)
- Um GID (grupo associado ao ficheiro)
- Os demais



Proteção de ficheiros no Linux: ACLs flexíveis (alguns FS)

ACL Básica pode ser aumentada com restrições granulares

- Por grupo ou utilizador
- **Necessita** de suporte do sistema de ficheiros
- Sobrepõem-se às ACLS do sistema
  - Presença de ACLs adicionais indicada com símbolo **+**

setfacl: permite adicionar ACLs

- Ex: setfacl –m u:www-data:rx fich
  - Define que o user www-data poderá ler e executar um ficheiro

getfacl: permite obter as ACLs de um ficheiro

- Ex: getfacl fich

Proteção de ficheiros no NTFS do Windows: ACLs de dimensão variável

Cada elemento do sistema de ficheiros possui uma ACL e um dono

- A ACL atribui 14 tipos de direitos a uma lista de entidades
- O dono pode ser um utilizador singular ou um grupo
- O dono não possui direitos especiais por esse facto

Entidades:

- Utilizadores singulares
- Grupos de utilizadores
  - Há um grupo, "Everyone", que representa "os demais"

- **Leitura**
  - listagem para diretorias
- **Escrita**
  - adição de ficheiros para diretorias
- **Execução**
  - uso como diretoria corrente para diretorias
- **Acrescento**
  - adição de subdiretorias para diretorias
- **Remoção de ficheiros e subdiretorias**
- **Remoção (do próprio)**
- **Leitura / escrita dos atributos**
- **Leitura dos atributos estendidos**
- **Leitura / alteração dos direitos**
- **Tomada de posse**

Elevação de privilégios: Mecanismo Set-UID

Esta funcionalidade serve para fazer uma alteração do UID do processo que executa um determinado programa

- Se um programa possuir o UID X e o bit set-UID activo na sua ACL, então ele será executado num processo com UID X independentemente do UID de quem o mandar executar

Na prática, esta funcionalidade serve para disponibilizar programas que realizam operações privilegiadas a utentes em quem não se confia

- Exemplo: alteração da senha do utente no ficheiro que guarda as senhas

Elevação de privilégios: Mecanismo sudo

A administração pelo root não é adequada

- Uma "identidade", muita gente
- Quem fez o quê?

Aproximação preferível

- Vários utilizadores podem ser administradores temporários
  - Usar temporariamente o UID 0
- sudo comando
  - Sudoers
  - Definido por um ficheiro de configuração usado pelo sudo

sudo é uma aplicação Set-UID com UID = 0

- Um registo adequado pode ser realizado por cada comando executado via sudo

Redução de privilégios: Mecanismo chroot

Permite diminuir a visibilidade do sistema de ficheiros

- Menor visibilidade, menor risco de ver o que não interessa

Cada descritor de processo possui o i-number do i-node raiz

- A partir do qual começa a resolução de nomes completos
  - /nome/nome/etc.

chroot permite mudar esse número para referir o i-node de outra diretoria arbitrária

- A vista do sistema de ficheiros do processo fica reduzida ao que existe abaixo dessa diretoria

É usado para proteger o sistema de ficheiros de aplicações potencialmente perigosas

- e.g. servidores públicos, aplicações descarregadas
- Mas é preciso ser usada com muito cuidado!